NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Percepções e comportamentos relativos a risco operacional

Estudo de uma Instituição Financeira Portuguesa

Luís Miguel Martins Antunes

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

Percepções e comportamentos relativos a risco operacional Estudo de uma Instituição Financeira Portuguesa

por

Luís Miguel Martins Antunes

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Gestão de Informação, Especialização em Gestão de Sistemas e Tecnologias de Informação

Orientador: Doutor Rui Alexandre Henriques Gonçalves

Novembro 2015

AGRADECIMENTOS

Quero agradecer à Instituição Financeira pela participação e disponibilização dos meios técnicos que contribuíram positivamente para a realização deste projecto.

Um agradecimento ao Dr. Luís Duarte, pelo conhecimento transmitido, pela confiança e apoio dado ao longo do meu percurso profissional e em particular neste projecto.

Um agradecimento muito especial ao Prof. Rui Gonçalves, pela orientação, apoio, partilha de ideias, de conhecimento e de sabedoria, os quais possibilitaram a realização e conclusão deste trabalho.

Agradeço aos meus pais todo o esforço, dedicação, motivação e carinho dado ao longo da minha vida.

Quero agradecer à minha esposa, Marisa, pelo apoio, compreensão e paciência, que foi determinante em todos os momentos do desenvolvimento da dissertação.

RESUMO

O factor humano é determinante para a eficácia da gestão do risco operacional, representando este factor, uma maior relevância, em instituições em que a recolha de eventos de risco operacional é maioritariamente um processo manual ou pouco automatizado, estando dependente em grande medida da boa vontade das pessoas em colaborar no processo. Este estudo tem como principal objectivo verificar a efectividade da metodologia vigente de disseminação e incorporação da gestão do risco operacional na cultura da instituição, através do estudo do comportamento e da percepção dos colaboradores para a temática do Risco Operacional. A metodologia de investigação utilizada assenta na revisão da literatura, num estudo de caso de uma instituição financeira portuguesa e num questionário dirigido ao universo de colaboradores da instituição, em particular aos colaboradores que desempenham funções de gestão intermédia e aqueles que estão na base da pirâmide hierárquica. Com base nos resultados obtidos, verificou-se a necessidade de elaborar um conjunto de recomendações com o objectivo de enriquecer a cultura de gestão de risco operacional e privilegiar a disseminação de conhecimento da temática.

PALAVRAS-CHAVE

Risco Operacional; Percepção; Comportamento; Cultura.

Códigos JEL: G21; G32; M14.

ABSTRACT

The human factor is crucial to the effectiveness of operational risk management, being this factor of greater relevance in institutions where the collection of operational risk incidents is done mostly as a manual or poorly automated process and is highly dependent upon the goodwill of people to cooperate in the process. This study aims to verify the effectiveness of the current methodology for the dissemination and incorporation of operational risk management the institution's culture, through the study of behaviour and perception of employees regarding operational risk. The research methodology used is based on literature review, a case study of a Portuguese financial institution and a questionnaire addressed to the institution's employees, particularly to those who perform middle management functions, as well as those that shape the foundations of the hierarchical pyramid of the organization. Based on the results achieved, there was the need to develop a set of recommendations in order to enrich the operational risk management culture and to privilege the knowledge dissemination towards the theme.

KEYWORDS

Operational Risk; Perception; Behaviour; Culture.

JEL Codes: G21; G32; M14.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

BCBS	Basel Committee on Banking Supervision
BdP	Banco de Portugal
BIS	Bank for International Settlements
CEBS	Committee of European Banking Supervisors
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
GRO	Gestor de Risco Operacional
Moody's	Moody's Invertor Service
RGICSF	Regime Geral das Instituições de Crédito e Sociedades Financeiras
RO	Risco Operacional
PwC	PricewaterhouseCoopers
WEF	World Economic Forum

1. INTRODUÇÃO

O risco, e em particular o risco operacional, esteve sempre presente na vida humana e associado às suas actividades. O risco, foi definido pela ISO 31000 como o efeito da incerteza nos objectivos, um desvio em relação ao esperado, é o estado de incerteza, ainda que parcial, da deficiência de informações relacionadas com a compreensão ou o conhecimento de um evento, da sua consequência ou probabilidade. Desde os primórdios dos tempos que o Homem, conseguiu ultrapassar as dificuldades e mitigar os riscos, mesmo que de forma inconsciente ou apenas por imposição da natureza. A adopção da posição erecta por parte do Homem primitivo proporcionou a mitigação de diversos riscos, permitindo-lhe observar e alcançar a partir de uma posição mais elevada, obter uma visão mais abrangente do meio envolvente, a detecção precoce de ameaças e ataques de outros animais, bem como a descoberta de alimentos essenciais para a sobrevivência da espécie (BdP, 2014). Em 1943, Abraham Maslow (Maslow, 1943), na sua pirâmide de necessidades (Figura 1.1) identificou, como uma das principais necessidades, a procura de segurança e estabilidade, a procura de coisas familiares em vez de estranhas, do conhecido em vez do desconhecido. O que está subjacente é a necessidade de retirar os riscos da obscuridade e alguma da sua incerteza, por forma a poder mitigá-los ou controlá-los. Segundo Bernstein (1998), o que define a fronteira entre os tempos modernos e o passado, é o domínio do risco, a noção de que o futuro é mais do que um capricho dos deuses e que os Homens não são passivos em relação à natureza. As bases da gestão dos riscos remonta a cerca de 3000 A.C., data na qual comerciantes chineses procuravam transferir e repartir o risco associado ao transporte marítimo de mercadorias, repartindo as mesmas por diversas embarcações afim de diminuir as perdas em caso de naufrágio (BdP, 2014).

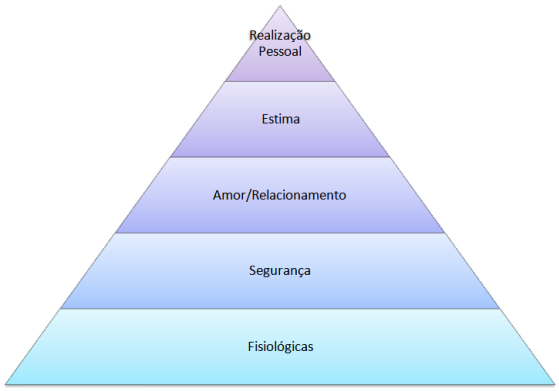

Figura 1.1 - Pirâmide de Necessidades

(Fonte: Maslow, 1943)

A gestão dos riscos, e em particular a gestão do risco operacional é transversal a qualquer actividade ou negócio. Vejamos o caso das Instituições Militares, a Indústria de Energia Nuclear, a Industria Aeronáutica (Doering, 2003), todas elas à largos anos deram grande enfoque à gestão deste tipo de risco. Uma das principais razões desta focalização poderá ser o facto do erro, ou do risco, estar

normalmente associado a perdas de vidas humanas, o que eleva esta temática para um patamar de superior importância.

Nas instituições financeiras, a temática do risco operacional, não sendo um tema novo, é certamente um tema actual. O risco foi sempre algo com que as instituições financeiras tiveram que lidar, uma vez que faz parte do seu negócio e portanto não pode ser totalmente eliminado. O que no presente se salienta é o interesse comum entre os bancos e a supervisão na identificação, medição, monitorização e controlo do risco operacional (Alexander, 2003).

Nos bancos em particular, a gestão de risco operacional é tão antiga quanto a sua criação (Hoffman, 2002). Inicialmente a gestão era focada para a protecção da moeda e dos metais preciosos de assaltos e roubos, presentemente, a evolução e maturação da gestão do risco operacional e da própria sociedade, provocou alterações no seu foco, continuando no entanto, fortemente associado ao comportamento humano e a ser uma parte importante e integrante do risco operacional, vejamos os casos de fraudes, transacções não autorizadas, ataques a sistemas de informação, falhas na garantia da continuidade do negócio, entre outros. Neste contexto, coloca-se a questão, se este tipo de risco sempre esteve presente na actividade bancária e o porquê de só na última década se ter dado maior importância ou relevância ao tema.

Inicialmente, as instituições financeiras e as entidades reguladoras consideraram, como sendo os riscos mais importantes, ou com maior probabilidade de causar impacto no capital das instituições, o risco de crédito (BCBS, 1988) e o risco de mercado (BCBS, 1995). Deixando o risco operacional como um risco multifacetado, não quantificável ou mensurável. O risco operacional era definido como qualquer risco que não se enquadrasse em risco de crédito e de mercado, o risco de perda decorrente de diversos tipos de erros humanos e técnicos, ou muito genericamente tratado como "outros riscos". (BCBS, 1998). A Figura 1.2 demonstra a visão anterior sobre o risco operacional como um risco residual ou complementar.

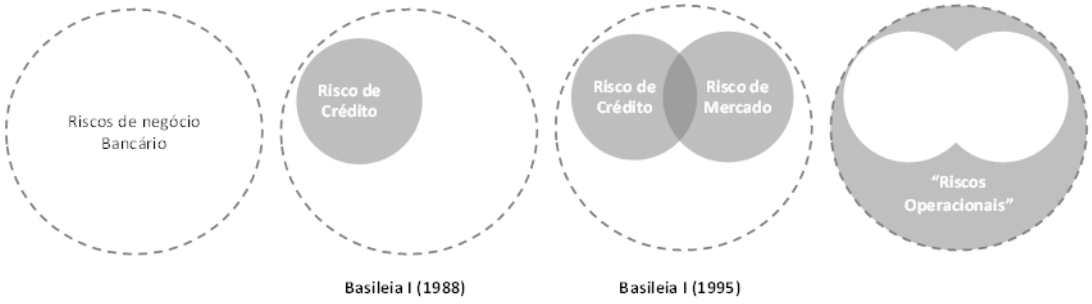

Figura 1.2 - Definição por exclusão, visão "negativa", do Risco Operacional

(Fonte: Nationalbank,2006)

Esta caracterização tornou difícil a sua identificação e medição, o que levou por vezes a que eventos de risco operacional fossem classificados erradamente como risco de mercado (caso Barings, transacções não autorizadas) ou como risco de crédito (caso Jurgen Schneider, obtenção de créditos com suporte a documentos falsos).

Em 2001, surgiu, através do *Bank for International Settlements*, e de acordo com proposta pela *British Bankers Association*, uma definição formal de risco operacional, como o risco de perda directa ou indirecta resultante de uma inadequação ou deficiência de procedimentos internos, de recursos humanos, de sistemas ou de acontecimentos externos (BCBS, 2001).

No entanto, já em 1998, o Comité de Basileia tinha elaborado um documento onde se destacavam uma das primeiras referências ao risco operacional, sendo definido como o risco de perdas potenciais relacionadas com deficiências de integridade e fiabilidade dos sistemas, considerando como fundamentais questões relacionadas com a segurança dos bancos, decorrente da sua propensão para ataques internos ou externos aos seus sistemas ou produtos. Estando igualmente exposto a abusos por parte dos clientes, da implementação ou concepção inadequado do sistema de banca electrónica, entre outros (BCBS, 1998).

Culp (2001) considera risco operacional, o risco de falhas com sistemas de informação, de supervisão e de controlos internos, ou de eventos decorrentes de desastres naturais e que irão impor perdas inesperadas em determinados processos da organização. Relaciona também as perdas com fraudes internas ou práticas comerciais inadequadas de empregados, ao desempenho de tarefas por colaboradores não qualificados para as efectuar, entre outros. O mesmo autor infere que no caso do risco operacional, as falhas em processos e de sistemas, tendem a surgir devido à falta, inadequada ou insuficiente atenção e percepção dos colaboradores no desempenho das suas funções ou pela definição errada ou insuficiente das suas responsabilidades. Globalmente as pessoas tendem a ser uma peça chave e a estar na raiz da grande maioria dos riscos operacionais.

Em 2004, o Acordo de Basileia II, veio enquadrar e clarificar a definição de risco operacional, como "o risco de perdas resultantes de uma inadequação ou deficiência de procedimentos, de recursos humanos, de sistemas, ou de acontecimentos externos, incluindo os riscos jurídicos, mas excluindo o risco estratégico e reputacional" (BCBS, 2004).

Na Figura 1.3 esquematiza-se esta nova visão positiva do risco operacional.

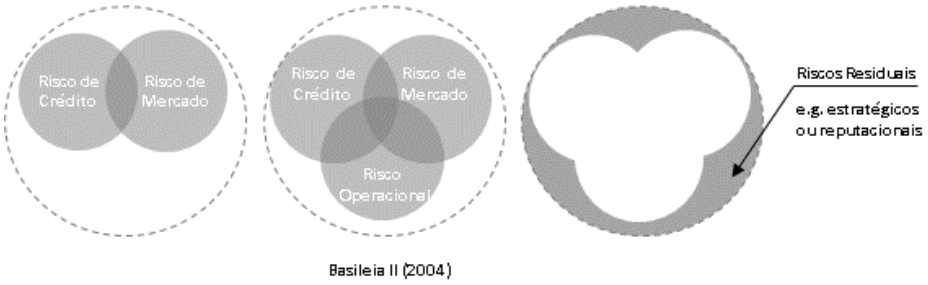

Figura 1.3 - Risco operacional definido como uma categoria de risco independente

(Fonte: Nationalbank, 2006)

Através deste novo paradigma, o risco operacional passou a ser alvo de uma maior atenção por parte das instituições financeiras e foco de maior investimento, com o intuito de reforçar a robustez e aumentar a eficácia da gestão do risco operacional.

1.1. RELEVÂNCIA DO TEMA

Decorrente da evolução da mentalidade dos conselhos de administração, dos gestores de topo, dos gestores de riscos, do desenvolvimento de sistemas de informação específicos para recolha de perdas de risco operacional e da crescente pressão das entidades de supervisão, a gestão de risco operacional tem alcançado uma maturidade e uma visibilidade crescente. Consequentemente (IBM, 2011), as instituições financeiras encetaram na procura da melhor forma de fomentar uma cultura de gestão de riscos a nível das áreas que desempenham funções de controlo (Função de Gestão de Riscos, Função de *Compliance* e Função de Auditoria Interna), na definição da estratégia de risco operacional com reflexo no desenho de perfis e na tolerância ao risco (Chorafas, 2003), no desenvolvimento de políticas, normas e procedimentos, bem como, incentivar uma cultura de gestão de riscos transversal a todas as unidades de negócio e colaboradores, estando integrada na sua actividade e rotina diária, e no âmbito das suas funções e competências.

Da observação da Figura 1.4, pode aferir-se que a identificação de riscos nas organizações, no que diz respeito aos colaboradores que desempenham funções de primeira linha, aqueles que por norma se encontram na base da hierarquia organizacional, tem uma expressão reduzida. Neste contexto, Chorafas (2003) realça como dificuldades no controlo do risco operacional, a falta de formação e inexperiência dos colaboradores e a falta de foco ou de linhas orientadoras, apresentando, igualmente, os constrangimentos para a sua colaboração: (i) os colaboradores não sabem qual o âmbito; (ii) os colaboradores não percebem como controlar o risco operacional; (iii) não pretendem fazê-lo de forma rigorosa, por forma a não ferir a sensibilidade de outras pessoas/colaboradores; (iv) não gostam de ser controladas.

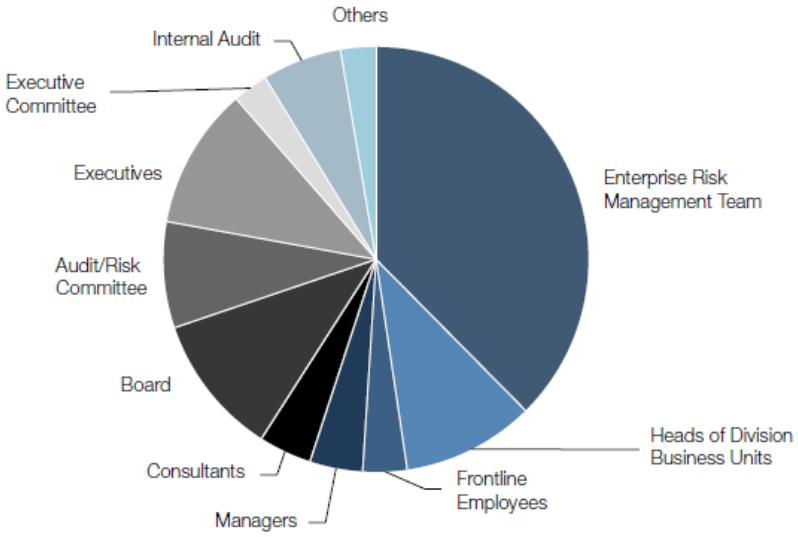

Figura 1.4- Quem está envolvido na identificação dos riscos

(Fonte: World Economic Forum, 2014)

No entanto, todas as áreas de uma organização que possam estar expostos a eventos de risco operacional, deverão ter consciência destes riscos e reportá-los, não apenas porque existem normas, políticas, regulamentos e controlos internos que as sujeita a cumprir determinados critérios e

comportamentos (World Economic Forum, 2014), mas porque existe uma cultura saudável de identificação e acompanhamento dos riscos. Desta forma, com a colaboração de toda a estrutura da organização, é espectável que a estratégia de gestão do risco seja eficaz, interdepartamental, que seja portadora de valor acrescentado e de vantagens competitivas.

Neste sentido, a gestão de topo tem que desempenhar um papel determinante na disseminação da cultura de gestão de riscos (BCBS, 2011). Por vezes o processo de gestão do risco desagrada aos colaboradores uma vez que é mais uma responsabilidade, para além das suas funções habituais ou porque apesar de contribuírem com informação, não recebem o devido *feedback*, situações que reflectem a cultura vigente (Culp, 2001). A gestão do risco está intimamente relacionada e tem que estar embebida no capital intelectual das instituições e no comportamento dos seus recursos humanos. A recolha e divulgação da informação deve ser oportuna, caso não aconteça, incorre-se no risco de estar sempre a "olhar para o espelho retrovisor" e a verificar apenas informação histórica. Se se elaborar relatórios sobre os riscos identificados numa base mensal, poderá significar que a informação reportada terá 30 dias de atraso, se pensarmos em reportes de informação trimestral, a situação afigura-se pior. Segundo Simon (2013), o comportamento e a percepção perante os riscos deve ser equiparado aos cuidados que qualquer pessoa tem no seu dia-a-dia. Por exemplo, para atravessar a estrada, um peão instintivamente verifica se existem perigos próximos, na actividade empresarial este instinto de identificação de riscos deve estar presente e integrado na cultura organizacional (Culp, 2001).

De acordo com um estudo realizado pela revista *Bank Director Magazine* (McCormick, 2013), foram questionados diversos membros da direcção e gestores de risco de instituições bancárias dos Estados Unidos da América com mais de $5 mil milhões de activos, sobre quais seriam os maiores desafios num programa empresarial de gestão de riscos. Ambos os inquiridos do estudo, afirmam que um dos maiores desafios são a criação de uma cultura que suporte a comunicação e avaliação de riscos transversalmente por toda a estrutura das instituições (Figura 1.5). Verifica-se que a questão cultural continua a ser um desafio em termos de gestão de riscos.

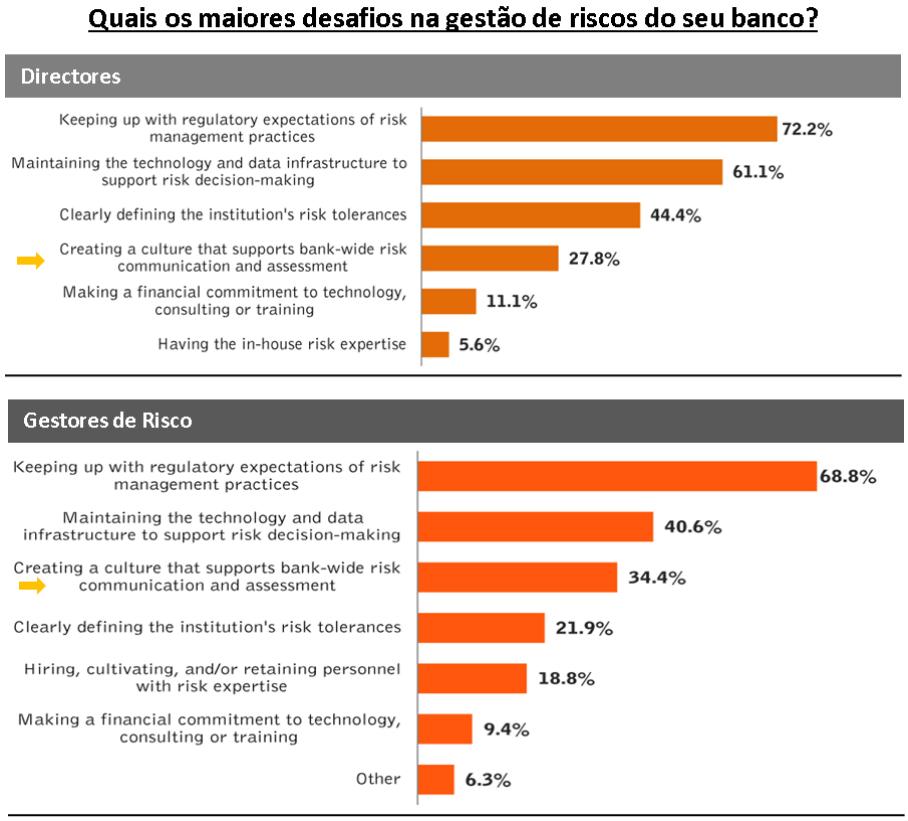

Figura 1.5 – Desafios na Gestão de Risco Operacional

(Fonte: McCormick, 2013)

Outrossim, perante a questão sobre com que categoria de risco está mais preocupado, é identificado pelos inquiridos, a categoria de risco operacional. Com base nos resultados obtidos no estudo, pode concluir-se que as instituições estão cientes dos desafios actuais do risco operacional, na relevância da promoção da gestão do conhecimento, na importância da comunicação de todas as fragilidades e de identificação de riscos por toda a estrutura organizacional (Figura 1.6).

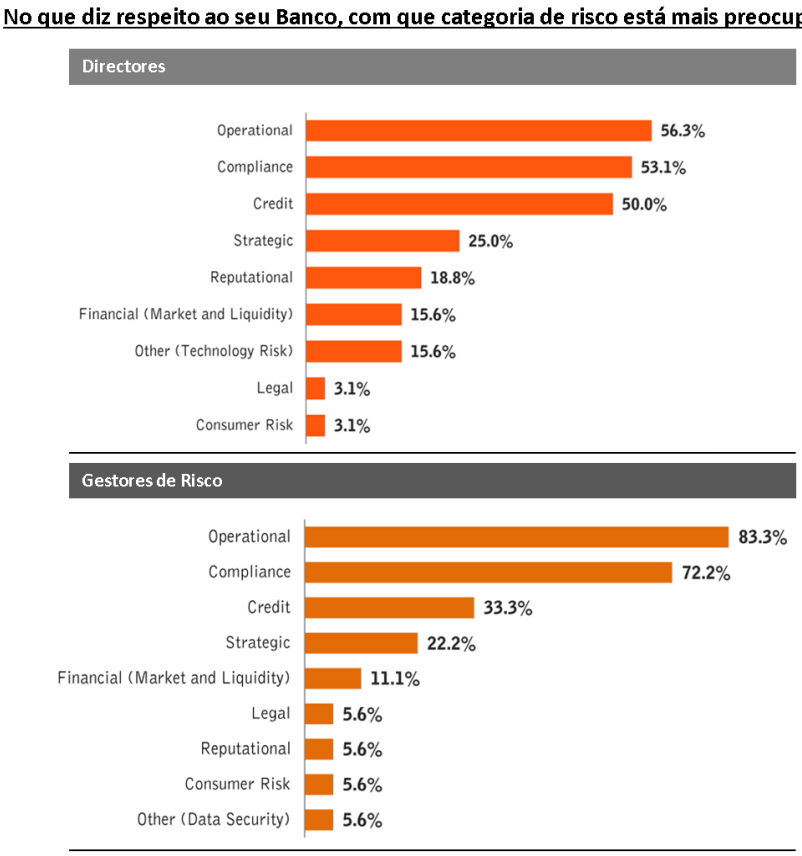

Figura 1.6 – Categorias de risco de acordo com a relevância

(Fonte: McCormick, 2013)

Por forma a demonstrar o impacto financeiro por perdas de risco operacional nas instituições, apresenta-se a Tabela 1.1, com casos de perdas mais significativos. Em resumo, de 1980 a 2000, a magnitude de perdas e impactos de riscos operacionais, que têm sido reveladas, atingem avultadas perdas, estimando-se que tenham um valor anual de $ 15 biliões (Hoffman, 2002).

Instituição Financeira	Descrição	Ano	Perda (Milhões $)
UBS	Manipulação da taxa libor	2015	1,4
Barclays	Diversos casos de manupulação de mercados: electricidade, ouro, taxa libor	2012 - 2014	1,4
Société Générale	Transações não autorizadas	2008	7,0
Sumitomo Corporation	Transacções fraudulentas	1986 - 1996	1,6
Suminot	Fraude, Falsificação e comercio não autorizado	1986 - 1996	1,7
Barings	Negociação e realização de transacções não autorizadas	1995	1,6
Daiwa Bank	Negociação e realização de transacções não autorizadas	1984 - 1995	1,1
US banks Corporation	Fraude de cheques	1993	12,0

Tabela 1.1 – Eventos mais conhecidos de risco operacional

(Fonte: Elaboração Própria)

No entanto, e uma vez que as perdas podem levar meses ou anos a se materializarem ou serem reconhecidas, é provável que muito eventos que estão neste momento a acontecer, ainda não estejam totalmente identificados ou descobertos e como tal, subavaliados (Chernobai, Jorion, & Yu, 2011).

1.2. QUESTÃO DE INVESTIGAÇÃO E OBJECTIVOS

Este trabalho de investigação tem como base de estudo uma Instituição Financeira portuguesa. O propósito principal da investigação é verificar se a metodologia vigente de disseminação e incorporação da gestão do risco operacional na cultura da instituição é efectiva, o qual será identificado através do estudo do comportamento e da percepção dos colaboradores para a temática do risco operacional.

De igual modo, e com o intuito de alcançar o objectivo global deste trabalho, será necessário aprofundar questões específicas que irão suportar e permitir responder claramente ao objectivo principal deste estudo:

- Conhecer as dificuldades inerentes à identificação, recolha e análise dos eventos de risco operacional detectadas, por parte dos diferentes níveis hierárquicos estudados;

- Avaliar o comportamento das áreas com funções de controlo perante o risco operacional, designadamente a função de *compliance*, a função de auditoria interna e a função de gestão de riscos;

- Verificar se existe uma percepção real para o que é, e o que representa, o risco operacional por parte das áreas comerciais da instituição financeira.

2. REVISÃO DA LITERATURA

De acordo com a Organização Internacional de Normalização[1], mais especificamente, a norma ISO 31000:2009, risco define-se como o efeito que a incerteza tem nos objectivos, sejam eles positivos ou negativos. Os riscos podem ser de diversas naturezas, riscos de mercados financeiros, riscos de falhas de projectos, riscos de crédito, riscos naturais, riscos operacionais, entre outros. O que todos têm em comum é o facto de o resultado do risco poder ser incontrolável e aleatório.

A palavra risco teve origem no século XVI e XVII e crê-se que remonta ou deriva do Português ou do Castelhano, sendo utilizado para se referir à incerteza inerente à navegação em águas desconhecidas. O termo nesta altura tinha uma conotação e estava associada a aspectos mais positivos, sendo referido e mencionado em oportunidades de negócio e de aspiração ao sucesso económico (BdP, 2014).

O principio fundamental do risco mantem-se (PwC, 2012), uma vez que, claramente a assunção de riscos sempre foi uma parte inerente/integrante dos negócios e quanto maior a apetência para o risco, mais se pode ganhar ou perder. Actualmente, o que mudou fundamentalmente, foi o quociente de risco necessário para alcançar o objectivo pretendido. Deste modo a gestão de riscos já não pode ser apenas uma reflexão sobre o passado, terá que ser uma parte integral da gestão estratégica. Presentemente, impera a imprevisibilidade e a volatilidade dos negócios e dos mercados, que requerem estratégias resilientes que possam adaptar-se à incerteza e à mudança. Um dos desafios é a definição e o desenvolvimento de uma *framework* de risco operacional que permita a atempada identificação de riscos operacionais, o seu controlo e mitigação e reflectir correctamente os níveis de risco operacional a que instituição está exposta (CEBS, 2006).

2.1. O RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS

Desde a definição, adopção e integração do conceito e da gestão do risco operacional nas instituições financeiras e nas entidades reguladores ou de supervisão, verifica-se que os mesmos têm evoluído, passando por vários níveis de maturidade, sendo o risco operacional, inicialmente, apenas considerado como um risco residual, até à sua sobrelevação a uma categoria de disciplina autónoma e distinta dos diversos riscos (CEBS, 2006). Ao logo do capítulo serão identificadas as perspectivas de diversas entidades no que diz respeito a esta temática.

Passados cerca de dez anos de críticas de diversos autores, verifica-se a existência de uma convergência no sentido de alterar o Acordo de Basileia II, no que diz respeito, entre outros, ao cálculo de requisitos de fundos próprios para risco operacional e a possível eliminação dos métodos de cálculo tendo por base uma percentagem fixa do indicador relevante ou o cálculo dos requisitos de fundos próprios, como uma determinada percentagem do indicador relevante por linha de negócio. Sendo transformados num novo Método Padrão Revisto (BCBS, 2014).

A evolução de mentalidade por parte das entidades reguladoras deveu-se a uma cada vez maior competitividade do mercado, à crescente complexidade dos produtos comercializados e ao facto de continuarem a ocorrer um número significativo de eventos relacionados com risco operacional (Davis, 2005).

[1] *International Organization for Standardization*

Contudo, já em 1999, a PwC (1999), decorrente da realização de um inquérito, identificou que a crescente atenção pelo risco operacional se deveu ao aumento do comprometimento da gestão de topo das instituições, o aumento da percepção sobre o risco operacional, uma resposta aos eventos internos e externos registados, o foco numa gestão dos riscos transversais a toda a organização e a atenção dada pelas entidades reguladores.

Do mesmo modo, Geiger (2002) reconhece que a crescente atenção das instituições financeiras para a gestão do risco operacional resultou de diversos factores, tais como, a percepção de que os riscos aumentaram significativamente nos últimos anos, a constatação das insuficiências que uma abordagem meramente quantitativa subjacente ao risco de crédito e de mercado, esconde riscos em áreas chave, e consequentemente, que a gestão do risco operacional deve ser desenvolvida e estudada de forma independente, bem como, o interesse crescente das autoridades de supervisão no risco operacional. Neste contexto, as instituições reguladoras do sector desempenharam o papel mais importante, indicando directrizes, regras, normas, bem como, métodos para cálculo de requisitos de capital, por forma a enfrentar o risco, caso este se materialize ou ocorra (BCSB, 2004). Para além das reformas regulatórias atuais, alguns especialistas acreditam que mudanças profundas na cultura e no sistema de incentivos das empresas do sector financeiro são necessários para reduzir a assunção de riscos excessivos (WEF, 2015).

Em resposta às crescentes dificuldades na gestão do risco operacional, ao crescente número de escândalos e perdas resultantes da exposição das instituições financeiras ao risco operacional, em 2001, foi publicado o documento consultivo, *Operational Risk –Supporting Document to the New Basel Capital Accord* (BCSB, 2001), em que se define o risco operacional como, "o risco de perdas directas ou indirectas, resultante da inadequação ou falha em processos internos, pessoas, sistemas e eventos externos", são igualmente definidas metodologias para cálculo de requisitos mínimos de capitais próprios para se enfrentar este risco e procede-se à definição de indicadores. Contudo, já em 1993, o *Group of Thirty*[2] no seu estudo *Global Derivates Study Group*, esboçou uma das mais reconhecidas definições para o risco operacional, o risco de perdas resultantes de sistemas e controlos inadequados, erros humanos e falhas na gestão. Caracterizando o risco operacional em 3 dimensões: Pessoas, Sistemas e Procedimentos ou Gestão.

Por seu lado, para Pyle (1997), o risco operacional resulta de perdas ou custos que advêm de erros na execução de operações e falhas no cumprimento da regulamentação vigente, identificando quatro fontes principais para a perda de valor nas instituições, o risco operacional, o risco de mercado, o risco de crédito e o risco de execução ou de cumprimento.

Doering (2003), sugere uma definição mais simplificada do risco operacional, definindo-o como o risco de impactos adversos no negócio quando levado a cabo de forma imprópria ou inadequada e pode resultar de factores externos. Afirmando que é o risco de não se fazerem "as coisas da forma correcta", e que tem como principal origem o interior da própria organização, com excepção dos eventos catalogados como eventos externos.

[2] *Group of Thirty* - Estabelecido em 1978, é uma organização internacional privada, sem fins lucrativos, composta por representantes dos sectores e universidades públicas e privadas. Destina-se a aprofundar a compreensão das questões económicas e financeiras internacionais, a explorar as repercussões internacionais das decisões tomadas nos sectores público e privado, e examinar as opções alternativas disponíveis para os operadores do mercado e os responsáveis políticos.

No contexto da definição emanada pelo Comité de Basileia, Brink (2002), Chernobai, Rachev e Fabozzi (2007) definem que o risco operacional é constituído por quatro dimensões, fontes de risco ou causas, as pessoas, os sistemas, os processos e riscos ou eventos externos, estando os mesmos implícitos na definição do risco operacional:

- Processos - Os processos numa instituição financeira podem ser simples, (o processo de deposito de numerário) ou processos complexos (a venda de produtos estruturados). Com a crescente complexidade de procedimentos e o maior número de processos, perdas podem ocorrer devido ao desenho errado ou falhas na sua aplicação. A implementação de procedimentos de controlos internos têm como objectivo evitar os erros e os riscos, no entanto, eles próprios podem conter riscos se forem incorrectamente desenhados e executados, tornando-se uma fonte de risco (Davis, 2005), uma vez que serão ineficientes (Davis, 2005). Independentemente da organização, os riscos estão embebidos nos seus processos, portanto não será suficiente apenas identificar e catalogar os riscos associados, mas sim, fazê-lo tendo presente os objectivos da instituição, focalizando-se e não dispersando recursos essenciais.

- Pessoas - Em termos de riscos operacionais associados a pessoas, estes podem ocorrer devido a diversos factores: a falta de conhecimento dos produtos da instituição; a grande pressão comercial para o cumprimento de objectivos; fraudes por parte dos empregados; segregação de funções, solicitando, por exemplo, à pessoa que controla um determinado processo, que o realize também. Hoje em dia, existem cada vez menos colaboradores em cada departamento ou secção, o que leva a que seja necessário trabalhar mais horas para além do tempo regulamentado, muitas vezes sem as devidas pausas para descanso, levando à fadiga física ou psicológica, e consequentemente, a que exista maior propensão para que sejam cometidos erros. Devido à cada vez maior complexidade de produtos e procedimentos (Brink, 2002), os colaboradores das instituições financeiras, terão dificuldades em conhecê-los em detalhe, podendo ser: inadvertidamente ou intencionalmente, a causa de um evento de risco operacional, ao não se aperceber da falta de conhecimento, agindo naturalmente pensando estar na posse de toda a informação; o colaborador reconhece a sua falta de conhecimento mas não se sente confortável para se expor e admitir que não está familiarizado com a tarefa ou com a situação; o colaborador tenta obter vantagens dessa falta de conhecimento, neste caso age com intenção, classificando-se como uma fraude interna.

- Sistemas - Relativamente aos riscos que podem advir desta dimensão, enquadram-se as falhas dos sistemas, riscos relacionados com as aplicações, com falhas de *hardware*, de armazenamento e de recuperação de dados, entre outros.

- Eventos Externos - As perdas que podem ocorrer de eventos externos englobam actos criminosos, desastres naturais, terrorismo, branqueamento de capitais, fraudes externas e fugas de informação por parte de empresas de *outsourcing*.

Já Akkizidis e Bouchereau (2006), afirmam que a crescente atenção para o risco operacional se deve a inúmeros factores, destacando-se o desenvolvimento de novos produtos e a sofisticação dos mesmos, novos canais de distribuição, novos mercados, novas tecnologias de informação interdependentes e complexas, o comércio electrónico, os tempos de processamento da informação, o volume de negócios, a globalização, a pressão dos accionistas, a pressão dos reguladores, fusões e aquisições, à diversidade cultural dos colaboradores e dos clientes, às agências de rating, o mercado de capitais e o terrorismo.

Na mesma vertente, Brink (2002) refere que diversos factores impactaram nas instituições financeiras, a liberalização e desregulamentação do mercado monetário e de capitais, a globalização, que originou a abertura dos mercados a novos concorrentes que anteriormente estavam confinados ao seu mercado local, levando a uma maior competição e internacionalização, criando por vezes choques culturais dentro das organizações. Estes choques culturais vão desde diferentes eficácias de medidas de controlo interno de acordo com a região do globo, uma vez que podem não ser compatíveis com a cultura local, a relação laboral entre as diferentes hierarquias das instituições e a própria segregação de funções pode ser díspar e ter uma aplicação distinta entre diferentes culturas, até à própria relação com os clientes. De igual modo, a internacionalização e a massificação da utilização de serviços bancários via *home banking* colocou uma grande pressão a nível dos sistemas de informação, das disponibilidades e de níveis de serviços, potenciando o surgimento de eventos de risco operacional. Da mesma forma, Davis (2005) afirma que, a exposição a este tipo de eventos de risco aumenta com o volume e a complexidade das transacções. Outro factor importante, é a sofisticação crescente dos produtos comercializados, de derivados, de produtos estruturados e complexos, com diversas opções e garantias associadas criando dificuldades adicionais no seu desenvolvimento, assim como, na definição e identificação dos riscos a estes associados.

Para Davis (2005), a dificuldade do risco operacional revela-se ao compararmos com outras categorias de risco. A nível do risco de crédito, sabe-se à partida os montantes de empréstimos efectuados e a quem, tendo-se uma aproximação da probabilidade de incumprimento através da análise dos proponentes e com suporte a modelos de *scoring*. No risco operacional estes modelos não têm capacidade para prever o risco ou grau de exposição ao risco (Chorafas, 2003). O facto de um processo nunca ter tido uma falha operacional, não se poderá considerar que está isento de riscos potenciais. No risco operacional, ao invés de outros tipos de risco, como é o caso do risco de mercado, a instituição financeira não obterá ganhos através de um maior ou menor apetite a este tipo de risco (Brink, 2002), o risco é assimétrico, causando principalmente perdas e não ganhos (Cummings, Lewis, & Wei, 2004). Enquanto que uma organização muitas vezes pode recuperar de eventos de risco de crédito e de mercado, no caso do risco operacional, esta recuperação pode ser impossível. Segundo Akkizidis e Bouchereau (2006), o risco apenas deve ser aceite quando os benefícios superam os custos. Os riscos operacionais apenas podem ser eliminados se a instituição deixar de existir. De acordo com o mesmos autores, os riscos de mercado e de crédito são externos, têm origem fora da organização e podem ser geradores ou impulsionadores de maiores receitas, por contraste os riscos operacionais não tem esta faceta, podendo também advir do interior da própria organização.

Grinsven (2009) acrescenta que os riscos operacionais podem ainda ter um impacto directo e visível em termos financeiros na instituição, ou indirectos, neste caso o impacto não é directamente visível.

Perdas de reputação ou falhas de segurança no local de trabalho, podem não ter impacto directo e visível quando ocorrem, no entanto, ao longo do tempo, podem causar perdas financeiras avultadas.

Com o intuito de reforçar a solidez e a estabilidade do sistema bancário, o Comité de Basileia considerou fundamental a revisão da *framework* de Basileia I, nesse sentido, em 2004, com a publicação do Acordo de Basileia ll, o risco operacional foi definido como o risco de perdas resultante de uma inadequação ou deficiência de procedimentos internos, de pessoal e de sistemas ou de acontecimentos externos. A definição inclui explicitamente os riscos legais, mas exclui os riscos estratégicos e reputacionais (BCSB, 2004). Deixando cair a referência às perdas indirectas para quantificação de requisitos de capital, uma vez que estes riscos são de difícil medição, no entanto, para referência interna, a exposição indirecta, tais como serviços, a reputação, a interrupção/continuidade do negócio, devem ser considerados dentro do âmbito (Culp, 2001).

Seguidamente, o BCBS (2004) caracteriza o risco operacional através de diferentes tipos de eventos, entre as quais se incluem: fraude interna; fraude externa; práticas em matéria de emprego e segurança no local de trabalho; clientes, produtos e práticas comerciais; danos ocasionais a activos físicos; perturbação das actividades comerciais e falhas de sistemas; execução, entrega e gestão de processos (Tabela 2.1).

Tipos de Evento de Risco Operacional	Definições
Fraude interna	Perdas decorrentes de actos destinados intencionalmente à prática de fraudes, à apropriação indevida de activos ou a contornar legislação, regulamentação ou políticas empresariais, com excepção de actos relacionados com a diferenciação/discriminação, que envolvam, pelo menos, uma parte interna da empresa
Fraude externa	Perdas decorrentes de actos destinados intencionalmente à prática de fraudes, à apropriação indevida de activos ou a contornar legislação por parte de um terceiro
Práticas em matéria de emprego e segurança no local de trabalho	Perdas decorrentes de actos que não se encontram em conformidade com legislação ou acordos de trabalho, saúde ou segurança, bem como do pagamento de danos pessoais ou de actos relacionados com a diferenciação/discriminação.
Clientes, produtos e práticas comerciais	Perdas decorrentes do incumprimento intencional ou por negligência de uma obrigação profissional relativamente a clientes específicos (incluindo requisitos fiduciários e de adequação) ou da natureza ou concepção de um produto.
Danos ocasionados a activos físicos	Perdas decorrentes de danos ou prejuízos causados a activos físicos por catástrofes naturais ou outros acontecimentos.
Perturbação das actividades comerciais e falhas do sistema	Perdas decorrentes da perturbação das actividades comerciais ou de falhas do sistema.
Execução, entrega e gestão de processos	Perdas decorrentes de falhas no processamento de operações ou na gestão de processos, bem como das relações com contrapartes comerciais e vendedores.

Tabela 2.1 - Tipos de Eventos de Risco Operacional

(Fonte: BdP, 2010 e BCBS, 2004)

Para Culp (2001), a definição do Comité de Basileia, é demasiado ambígua, indicando que a distinção entre o risco operacional e o risco de negócio dependente da própria estratégia de negócio. A falência de um grande devedor pode constituir uma falha do sistema de controlo da instituição, ou no caso de uma empresa de recuperação de créditos pode representar apenas um risco do negócio. Por outro lado, Buchelt e Unteregger (2004), entendem que se deve lidar com o risco operacional, dada a sua natureza, de forma diferente do risco de crédito e de mercado. Neste contexto, e dada a abrangência do termo, o risco operacional pode ser classificado como um risco de cultura organizacional, considerando que lida com um conjunto de riscos variados, interrelacionados e com diferentes origens. A gestão deste risco tem necessariamente que ser efectuado a nível global por toda a organização, com o apoio da gestão e suportada por uma comunicação eficiente.

Em linha com o pensamento exposto anteriormente, a PwC (2005) invoca que a evolução da gestão do risco operacional tem sido travada pela falha na integração do risco operacional na gestão global de riscos (Figura 2.1).

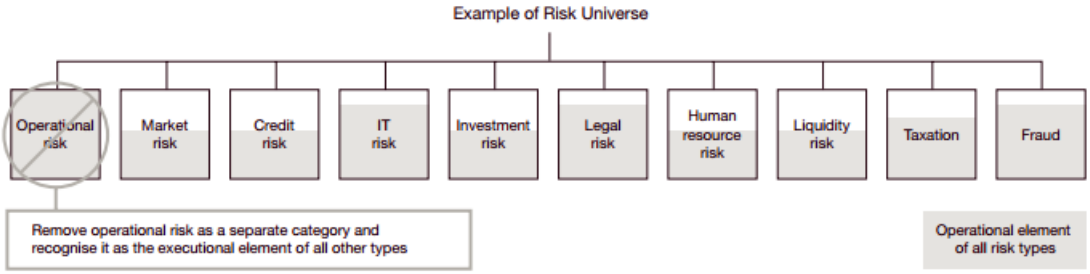

Figura 2.1 – Integração do risco operacional noutras categorias de risco

(Fonte: PwC, 2005)

O risco operacional é muitas vezes visto isoladamente, em vez de parte integrante de todos os outros tipos de risco. Levando à percepção de que o processo de risco operacional é uma duplicação desnecessária de controlos e sem ligação à realidade (PwC, 2005).

O Banco de Portugal (2014), apresenta uma definição em linha com a proposta por Basileia, define-se como o risco de perdas ou impactos negativos financeiros, no negócio ou na imagem/reputação da organização, causados por falhas ou deficiências na governação e processos de negócio, nas pessoas, nos sistemas ou resultantes de eventos externos, que poderão ser despoletados por uma multiplicidade de eventos. Em seguida, na Figura 2.2 esquematiza-se esta visão do Risco Operacional na qual incorpora eventos, causas e impactos.

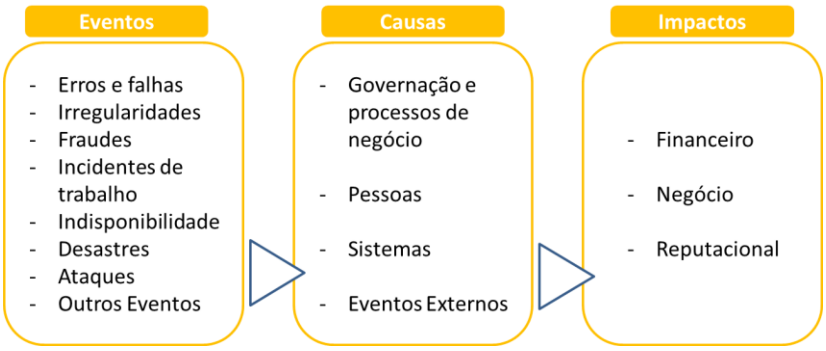

Figura 2.2 – Âmbito do risco operacional

(Fonte: BdP, 2014)

Importa agora detalhar a *framework* do Acordo de Basileia II no que diz respeito aos seus pilares fundamentais. O documento encontra-se estruturado e subdividido por 3 pilares interligados, que em conjunto contribuem para a solidez e robustez do sistema financeiro: 1º Pilar - Requisitos mínimos de capital; 2º Pilar - Processo de Avaliação pela Autoridade de Supervisão; 3º Pilar - Disciplina de mercado. Em seguida, na Figura 2.3, são apresentados os pilares fundamentais do Acordo de Basileia ll, e mais detalhadamente o 1º Pilar.

Figura 2.3 - Métodos de alocação de capital

(Fonte: Carvalho & Marcelo, 2008)

No primeiro pilar são definidos os requisitos mínimos de capital para a cobertura dos riscos de crédito, de mercado e operacional e são definidas as condições de utilização das diversas metodologias para o cálculo dos requisitos de fundos próprios para os três riscos mencionados.

O Acordo de Basileia, coloca três formas diferentes para efectuar este cálculo, deixando ao critério de cada instituição qual utilizar, impondo que a partir do momento em que utilizem um método mais sofisticado, não podem voltar para outro que tenha menor grau de sofisticação. Excepto se a entidade de supervisão entender que já não são cumpridos os critérios de elegibilidade ou qualificação para a utilização de determinado método, pode a mesma exigir que a instituição reverta para uma abordagem mais simples para todas ou algumas das suas operações. Por ordem crescente de complexidade os métodos são: o Método Básico, o Método Padrão ou *Standard* e o Método de Medição Avançado. Os métodos apresentam um crescente nível de complexidade, de requisitos qualitativos e quantitativos e de detalhe. As instituições são incentivadas e encorajadas a evoluir no espectro das abordagens disponíveis ao desenvolverem práticas e sistemas de medição de risco operacional mais sofisticados. Consequentemente, têm a possibilidade de reduzir os requisitos de fundos próprios para a cobertura do risco operacional ao adoptarem métodos mais avançados. A Figura 2.4, esquematiza o exposto anteriormente, caracterizando as três abordagens pelo nível de exactidão, o nível de requisitos qualitativos, a simplicidade do método, a granularidade e a sensibilidade ao risco.

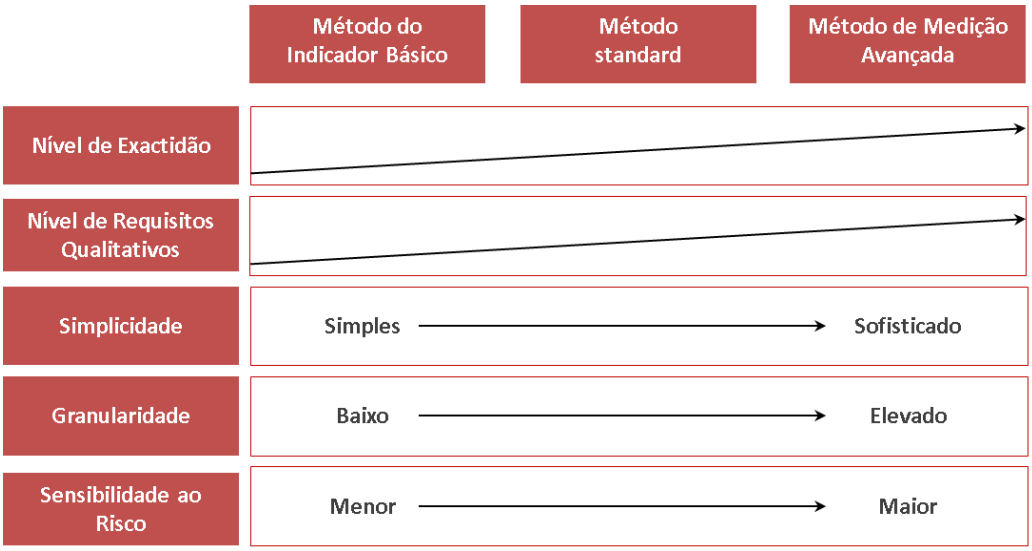

Figura 2.4 – Caracterização das abordagens de cálculo dos requisitos de fundos próprios

(Fonte: Elaboração própria com consulta de PwC, 2006, Crouchy, Galai & Mark, 2003, e BCBS, 2004)

O Método do Indicador Básico (BIA) é baseado num indicador percentual fixo (BdP, 2007) e os requisitos de fundos próprios para a cobertura de risco operacional correspondem a 15% da média dos últimos três anos do indicador relevante anual positivo. O indicador relevante é o resultado da soma líquida de juros com outras receitas líquidas e os resultados brutos de exploração, numa base anual (Tabela 2.2). Caso a soma da margem líquida seja negativa ou igual a zero em alguns dos anos, este não deve ser considerado no cálculo da média dos três últimos anos.

Elementos constituintes do Indicador Relevante
+ Receitas de juros e proveitos equiparados - Encargos com juros e custos equiparados
+ Receitas de acções e outros títulos de rendimento variável/fixo
+ Comissões recebidas - Comissões pagas
+ Resultados provenientes de operações financeiras
+ Outros proveitos de exploração

Tabela 2.2 – Elementos constituintes do Indicador Relevante

(Fonte: BdP, 2007)

Alexander (2003) refuta que a utilização de tal indicador é no mínimo discutível, uma vez que associar o indicador relevante ao risco operacional das instituições, não é realista e não reflecte a verdadeira exposição ao risco, é apenas um indicador razoável da dimensão das actividades da instituição, no entanto, também argumenta que não existem muitos indicadores alternativos e que são difíceis de definir. Por fim, concorda que o indicador relevante é a opção que menos desvantagens trás ao processo, por estar facilmente disponível, verificável e comparável por várias instituições sediadas em diversas partes do globo.

Para Chernobai et al., (2007), as vantagens deste método são a simplicidade da sua implementação, é útil como base inicial para a implementação de Basileia II, em especial quando os dados referentes a perdas são insuficientes para a utilização de modelos mais complexos, e é particularmente aplicável a instituições de pequena e média dimensão. No entanto, apresenta também alguns inconvenientes desta abordagem, o método não tem em conta a especificidade da instituição perante o risco operacional no que diz respeito à sua exposição, à estrutura das actividades de negócio, ao *rating* de crédito e outros indicadores, não representando o perfil e a sensibilidade a este risco, muitas vezes, resulta de uma sobreavaliação das verdadeiras necessidades de capital alocados ao risco, não sendo aplicável a bancos de grande dimensão e que tenham expressão internacional.

Nesta abordagem, não são especificados critérios de elegibilidade específicos, no entanto, os bancos são encorajados a respeitar as melhores práticas definidas pelo Comité de Basileia para a gestão do risco operacional.

No Método *Standard* (TSA), os requisitos de fundos próprios para a cobertura de risco operacional consistem na média dos últimos três anos da soma dos indicadores relevantes ponderados pelo risco, calculado em cada ano, relativamente aos oito segmentos de actividade (Tabela 2.2). Sempre que os capitais próprios sejam globalmente negativos em todos os segmentos de actividade num determinado ano, os dados a introduzir para a média relativa a esse ano serão zero. Neste âmbito existe ainda o Método *Standard* Alternativo (ASA), que difere do *standard*, no que diz respeito a duas das linhas de negócio, a banca de retalho e a comercial, sendo utilizada uma medida de exposição ao invés do indicador utilizado no método *standard*. O método apresenta vantagens adicionais, comparativamente com o método básico, apresentando-se mais preciso nos cálculos de requisitos de capital, uma vez diferencia a exposição ao risco operacional por linha de negócio. No entanto, ao apresentar indicadores fixos por linha de negócio, não tem em conta as especificidades das mesmas em cada instituição, da utilização do método, pode também resultar uma sobreavaliação das verdadeiras necessidades de capital alocados ao risco e não deve ser aplicável a bancos de grande dimensão e que tenham expressão internacional (Chernobai et al, 2007).

Segmentos de Actividade	Factores de Risco
Financiamento das empresas (corporate finance)	18 %
Negociação e vendas	18%
Pagamento e liquidação	18 %
Banca comercial	15 %
Serviços de agência	15 %
Banca de retalho	12%
Intermediação relativa à carteira de retalho	12 %
Gestão de activos	12 %

Tabela 2.3 – Segmentos de actividade/Linhas de Negócio

(Fonte: BdP ,2010)

No que diz respeito ao Método de Medição Avançado (AMA), a determinação dos requisitos de fundos próprios para a cobertura de risco operacional baseia-se nos sistemas de medição interna da instituição e está sujeito à aprovação pela entidade reguladora. O método permite que existam um conjunto alargado de abordagens na medição do risco operacional, sendo indicados critérios de elegibilidade, tanto a nível quantitativo, como a nível qualitativo, é dada a possibilidade de ver reflectido o impacto dos seguros e de outros mecanismos de transferência de risco, de forma positiva, para o cálculo requisitos de fundos próprios. O método pode ser utilizado de forma parcial em partes das actividades e nas restantes o indicador básico ou o *standard*. Na Tabela 2.3, exibe-se um resumo dos principais aspectos a considerar para elegibilidade aos diferentes métodos para cálculo de requisitos de fundos próprios para cobertura de risco operacional.

Principais Critérios	BIA	TSA	AMA
Cumprimento das "Sound Practices for the Management and Supervision of Operational Risk". [3]	-	x	x
Apresentar dispositivos sólidos em matéria de governo da sociedade, incluindo uma estrutura organizativa clara, com linhas de responsabilidade bem definidas, transparentes e coerentes.[4]	-	x	x
Organizar processos eficazes de identificação, gestão, controlo e comunicação dos riscos a que está ou possa vir a estar exposta.[4]	-	x	x
Dispor de mecanismos adequados de controlo interno, incluindo procedimentos administrativos e contabilísticos sólidos. [4]	-	x	x
Registo de perdas por segmentos de actividade/linhas de negócio, desenvolver políticas e documentação descrevendo os critérios de mapeamento do indicador relevante por linha de negócio.	-	x	x
Existência de recursos suficientes na utilização da abordagem nas principais linhas de negócio bem como nas áreas de controlo e de auditoria.	-	x	x
Existência de reportes regulares relativamente à exposição ao risco operacional, incluindo perdas materiais, destinados às funções e órgãos internos relevantes, bem como, aos órgãos de direcção e de administração. Assegurar a tomada de acções apropriadas de acordo com a informação reportada.	-	x	x
Existência de um sistema de gestão de risco operacional conceptualmente são, aplicado com integridade, bem documentado, e o sistema de medição deve ser parte integrante da rotina do processo de gestão de riscos.	-	x	x
O banco deve ter um sistema de gestão do risco operacional com atribuições claras de responsabilidades à uma função de gestão do risco operacional.	-	x	x
Conselho de administração e a gestão de topo, activamente envolvidos na supervisão da *framework* de gestão de risco operacional	-	x	x
O processo de gestão do risco operacional do banco e o sistema de avaliação deve ser objecto de validação e de revisão regular independente, auditores externos e supervisores.	-	x	x
Está sujeita a aprovação por parte das entidades de supervisão.	-	x	x
O sistema de medição do risco operacional deve ter em linha de conta ou integrar o uso de dados internos, informação externa relevante, análise de cenários, indicadores que reflictam o ambiente do negócio e do sistema de controlo interno.	-	-	x
As medidas do risco operacional geradas internamente e para fins de cálculo do capital regulamentar, devem basear-se num histórico de observações mínimo de cinco anos. Três anos no primeiro ano de adopção do AMA.	-	-	x
O banco deve ter uma função de gestão do risco operacional independente e que é responsável pela concepção e implementação da framework de gestão do risco operacional.	-	-	x
As instituições devem recolher informações acerca da data do acontecimento, quaisquer recuperações de montantes brutos de perdas, bem como informações descritivas quanto aos factores ou causas subjacentes ao acontecimento relativo às perdas, e de acordo os tipos de eventos de risco operacional.	-	-	x
Permite a redução dos requisitos de fundos próprios decorrente do reconhecimento dos seguros e de outros mecanismos de transferência de risco	-	-	x

Tabela 2.4 - Principais Critérios de qualificação para utilização dos Métodos BIA, TSA e AMA

(Fonte: Elaboração própria com consulta de BdP, 2007 e BCBS,2004)

Contudo, Sundmacher (2007) entende e demonstra que existem poucos incentivos para as instituições avançarem e evoluírem no expecto de abordagens definidas pelo Comité de Basileia, do mesmo modo, o cálculo de capital alocado ao risco operacional, não permite identificar as causas das perdas de risco operacional.

[3] Recomendado no método básico.

[4] Alineas f) a h) do artigo 14.º e alinea f) do artigo 17.º do Regime geral das Instituições de Crédito e Sociedades Financeiras (RGICSF).

No que diz respeito ao Pilar 2, este apresenta os princípios-chave de resposta da entidade supervisora ao primeiro pilar, a transparência na supervisão e orientações para a gestão de riscos, incluindo todos os outros riscos que um banco pode enfrentar, como o risco sistémico, o risco estratégico, o risco da reputação, o risco de liquidez e o risco legal. O Comité de Basileia entende, no entanto, que estes riscos apesar de difícil mensuração, não deve ser impeditivo para as instituições desenvolverem técnicas para os gerir. Destina-se não só a garantir que os bancos tenham capital adequado para reforçar a ligação entre o capital interno detido por uma instituição e os riscos emergentes da sua actividade, bem como encorajar os bancos a desenvolver técnicas e processos de gestão de riscos adequados, que permitam identificar, medir, agregar e monitorizar os riscos (CEBS, 2006).

De igual modo, o processo de supervisão define como as instituições devem cumprir com as orientações de governo interno e com o nível de capital interno adequado aos riscos decorrentes da respectiva actividade (o designado ICAAP – *Internal Adequacy Assessment Process*). No âmbito da estrutura de governo interno, o ICAAP é um processo que permite assegurar ao órgão de administração:

- Identificar, medir, agregar e monitorizar os riscos da instituição;
- Manter o capital interno adequado relativamente ao perfil de risco da instituição;
- Procurar a melhoria contínua do sistema de gestão de riscos.

No que concerne à regulamentação a nível nacional, o modelo de avaliação de riscos (MAR) foi o modelo desenvolvido e adoptado pelo Banco de Portugal no âmbito do Processo de Supervisão. Neste sentido, cabe ao Banco de Portugal, enquanto autoridade de supervisão e tal como estabelecido no artigo n.º 116.º-A do RGICSF, a responsabilidade de efectuar a sua própria avaliação da magnitude dos riscos subjacentes às actividades das instituições e verificar se os dispositivos em matéria de governo interno da sociedade, os pressupostos e resultados do ICAAP, bem como, os fundos próprios existentes, garantem uma adequada cobertura dos riscos. O MAR baseia-se nas recomendações do Comité de Basileia e do Comité de Supervisores Bancários Europeus (CEBS), nomeadamente as divulgadas através das "*Guidelines on the Application of the Supervisory Review Process under Pillar 2*" (CEBS, 2006), sobre os princípios a respeitar pelos sistemas de avaliação de riscos a utilizar pelas autoridades de supervisão no âmbito do Processo de Supervisão.

O Pilar 2 assenta em quatro princípios fundamentais:

- Princípio 1 - As Instituições financeiras devem possuir um processo que lhes permita avaliar a adequação de capital em relação ao seu perfil de risco e ter uma estratégia adequada por forma a manter os seus níveis de capital;

- Princípio 2 - Os supervisores devem rever regularmente o processo interno de avaliação da adequação de capital das instituições financeiras e as estratégias, bem como, a sua capacidade para monitorar e garantir a conformidade com os rácios de capital regulamentares;

- Princípio 3 - Os supervisores devem esperar que as instituições financeiras operem acima do nível mínimo de capital regulamentar e deverão ter a capacidade para impor que as instituições financeiras mantenham níveis de capital acima do mínimo legal;

- Princípio 4 - Os supervisores devem procurar intervir antecipadamente por forma a prevenir que os níveis mínimos de capital necessários para suportar os riscos incorridos sejam menores do que o requerido, devem também aplicar medidas correctivas sempre que o capital não seja mantido ou reposto.

Neste Pilar, e no que diz respeito ao risco operacional, é realçado que o indicador relevante utilizado nas metodologias básica e *standard* é apenas um indicador que representa a escala de exposição ao risco operacional, e pode em alguns casos ser uma subestimação para as necessidade de capital para enfrentar este risco (em casos de bancos com baixas margens ou rentabilidade). Podendo o supervisor aferir da adequabilidade dos resultados obtidos através do Pilar 1, relativamente à exposição ao risco.

Os bancos devem portanto, ter um processo para avaliar a sua adequação de capital global em relação ao seu perfil de risco e uma estratégia para manter os seus níveis de capital, bem como, desenvolver políticas que permitam delinear a estratégia de identificação, avaliação, monitorização e de controlo e mitigação do risco.

Por fim, o terceiro pilar tem como objectivo complementar os dois primeiros pilares e estabelece os requisitos de divulgação de informação aos mercados, investidores e ao público em geral, pretende assegurar uma maior transparência no que respeita ao perfil de risco, a adequação do capital das instituições financeiras e assegurar uma efectiva disciplina de mercado. Esta é exercida através da monitorização e avaliação pelos participantes no mercado, nomeadamente, outras instituições, clientes, contrapartes e investidores, da informação tornada pública sobre a solvabilidade e o perfil de risco das instituições.

Em 2010 e após a crise económica e financeira de 2007, que impactou no sector financeiro, o Comité de Basileia publicou o Acordo de Basileia III, com o intuito de reforçar e fortalecer a resiliência do sector e aumentar a capacidade de absorção de impactos em tempos de stresse financeiro e económico, reduzindo assim o risco de existirem repercussões e de contágio do sector financeiro para a economia real, aprimorar as práticas de gestão e governação de riscos, assim como, aumentar a transparência e as boas práticas de divulgação da informação (PwC, 2013). O documento introduz na *framework* um conjunto de elementos macro prudenciais, por forma a conter o risco sistémico de futuros impactos negativos entre instituições financeiras: (i) Aumentar a qualidade, consistência e transparência da base de capital; (ii) Reforçar a cobertura de risco; (iii) Completar as exigências de capital com um rácio de alavancagem; (iv) Reduzir a pró-ciclicidade e promover *buffers* ou almofadas contracíclicas; (v) Abordar o risco sistémico e a interligação ou interdependência entre as instituições.

Passada uma década sobre Basileia II, e em consequência da referida crise financeira e das fragilidades identificadas, mas também, da experiência obtida na implementação da *framework* de risco operacional, o Comité de Basileia tem vindo a rever os requisitos de fundos próprios previstos no Pilar 1 de Basileia II. Os requisitos de capital, nos métodos mais básicos (BIA, TSA, ASA), e apesar do aumento do número e da severidade de eventos de risco operacional, mantiveram-se constante

ou diminuíram. Tal como referido anteriormente, Alexander (2003) e Chernobai et al. (2007), indicam que a existência de um conjunto de abordagens simples, não estimam correctamente os requisitos de fundos próprios para o risco operacional. Esta fragilidade resulta principalmente do uso do indicador relevante, como indicador de exposição ao risco assumindo que este está directamente relacionado com o aumento do volume e das receitas de negócio.

Espelhando esta preocupação, o Comité de Basileia (BCBS, 2014) elaborou o documento consultivo – *Operational risk - Revisions to the simpler approaches*, no qual aborda o Método *Standard* revisto (SA), com a perspectiva de melhorar e colmatar os pontos fracos dos métodos mais básicos, substituindo o indicador anterior por um mais relevante (o indicador de negócio- BI), e melhorar a calibração dos coeficientes regulamentares (BIA – alfa, TSA - betas), baseando-se numa análise quantitativa. O indicador é o resultado da soma de três macro componentes da receita da instituição, a componente dos juros, a componente dos serviços e a componente financeira. Tratando-se de um documento consultivo, não existe até ao final do primeiro semestre de 2015, uma versão final e definitiva do novo método, bem como, do novo indicador a utilizar para cálculo dos requisitos de capital.

2.2. PERCEPÇÃO E GESTÃO DO RISCO OPERACIONAL

A má gestão e uma liderança frágil pode levar a uma "cultura da culpa", resultando na ocultação de deficiências ou fragilidades identificadas, no encobrimento de falhas e de perdas potenciais (Moody's, 2004). Ao longo deste capítulo serão verificados os aspectos fundamentais e o impacto que a percepção do risco operacional tem numa efectiva, sólida e abrangente gestão do risco operacional, bem como, os comportamentos que a condicionam ou influenciam.

O sector financeiro tem visto avanços consideráveis no domínio da gestão de riscos, com o risco operacional a receber maior destaque e ser a reconhecido como uma categoria de risco própria. Um número significativo de perdas com grande impacto financeiro, alguns dos quais colocando em causa a continuidade de algumas instituições, demonstraram claramente a importância da gestão do risco operacional (BdP, 2014).

Marshal (2001), entende que a gestão do risco operacional compreende uma série de actividades: a identificação do risco; a medição do risco; a prevenção de perdas operacionais; reduzindo a sensibilidade da instituição a eventos, através de planos de continuidade de negócio, de contingência e de continuidade de operações, que permitam a recuperação do negócio e das funções críticas em caso de ocorrência de desastres, por forma a não colocar em causa a sobrevivência da instituição; prever perdas potenciais; transferir o risco para entidades externas, tal como, seguradoras; transformar um determinado tipo de risco, noutro e mitigá-lo; e por fim alocar capital por forma a cobrir perdas de risco operacional. Complementarmente, o BdP (2007) indica que devem vigorar políticas e procedimentos destinados a avaliar e a gerir a sujeição ao risco operacional, incluindo para acontecimentos de reduzida frequência, mas de grande impacto, elaboração de planos de emergência e de continuidade da actividade a fim de assegurar a capacidade das instituições operarem numa base contínua e tendo em vista a contenção de perdas na eventualidade de uma perturbação grave das actividades. As remunerações e a política de incentivos devem promover e ser coerentes com uma gestão de riscos sã e prudente e não deve incentivar a assunção de riscos em níveis superiores ao risco tolerado pela instituição.

Neste contexto, as instituições financeiras deverão adoptar um conjunto de medidas que visem o acompanhamento e controlo do risco operacional, para tal, em 2003, o Comité de Basileia produziu o documento "*Sound Practices for the Management and Supervision of Operational Risk* " (BCBS, 2003), com um conjunto de práticas que os bancos deverão implementar de forma a gerirem melhor o seu risco operacional, definindo como aspectos fulcrais uma comunicação interna eficaz, a implementação de planos de contingência, uma forte cultura de controlo interno e de risco operacional. Esta cultura reflecte um conjunto combinado de valores individuais e corporativos, atitudes, competências e comportamentos que determinam o compromisso da instituição perante a gestão do risco operacional. Como parte do pilar II do Acordo de Basileia e em sequência da evolução do conhecimento e da experiência na implementação de um sistema de gestão do risco operacional, o Comité de Basileia (BCBS, 2014), apresentou um conjunto de medidas nas quais se dá enfâse ao desenvolvimento de um ambiente de gestão de riscos adequado:

1. O conselho de administração e a gestão de topo devem estabelecer uma forte cultura organizacional de gestão de riscos, que suporte e providencie comportamentos responsáveis. É da responsabilidade do conselho de administração assegurar que esta cultura é seguida por toda a organização, que é mantido um código de conduta, que defina com clareza padrões de integridade e de elevados padrões de ética, bem como a definição das melhores práticas de negócio.

2. Os bancos devem desenvolver, implementar e manter uma *framework* que é integrada no processo global de gestão de riscos.

3. O conselho de administração deve estabelecer, aprovar e rever periodicamente a *framework*. Deve também supervisionar os gestores de topo, por forma a assegurar que as políticas, processos e sistemas são implementados eficientemente a todos os níveis da instituição.

4. O conselho de administração deve aprovar e rever o apetite e tolerância ao risco operacional, articulado com a natureza, tipos e níveis de risco operacional a que o banco está disposto a assumir.

5. A gestão de topo deve desenvolver e propor ao conselho de administração, um claro, efectivo e robusto sistema de governação, bem definido, transparente e consistente com os níveis de responsabilidade.

6. A gestão de topo deve assegurar a identificação e avaliação do risco operacional inerente a todos os produtos, actividades, processos e sistemas, de modo a garantir que os riscos são bem conhecidos.

7. A gestão de topo deve assegurar que existe um processo de aprovação para todos os novos produtos, actividades, processos, e sistemas, que avaliem totalmente o risco operacional.

8. A gestão de topo deve implementar um processo que monitorize regularmente, o perfil e a exposição ao risco operacional, por forma a suportar uma gestão proactivo do risco operacional.

9. Os bancos devem ter um forte ambiente de controlo ao nível das políticas, processos e sistemas, bem como, um apropriado sistema de controlo interno e definição de estratégias de transferência e/ou de mitigação dos riscos.

10. Os bancos devem ter planos de continuidade de negócio, que permitam garantir a resiliência da instituição, visando assegurar o funcionamento contínuo da mesma e limitar as perdas, em caso de ocorrências susceptível de perturbar o normal desenrolar do negócio.

11. A divulgação e reporte público devem permitir que os accionistas avaliem a abordagem da instituição à gestão do risco operacional.

Dando ênfase e reforçando o referido anteriormente, apresenta-se o Aviso n.º5/2008 do Banco de Portugal no qual se evidência que: (i) a cultura organizacional da instituição deve garantir que todos os colaboradores reconhecem a importância do controlo interno, de modo a assegurar uma gestão sã e prudente da actividade da instituição; (ii) a cultura organizacional deve alicerçar-se em elevados padrões de ética, integridade e profissionalismo, os quais devem estar formalizados em códigos de conduta aplicáveis a todos os colaboradores da instituição; (iii) todos os colaboradores da instituição devem contribuir para o controlo interno, devendo, para o efeito, compreender o seu papel no sistema implementado.

Neste contexto, Young e Coleman (2009) identificam dois aspectos fundamentais nos quais se deve apoiar a gestão dos riscos, a liderança e a eficácia e eficiência das organizações. A qualidade da gestão e a liderança são considerados pontos-chave, incluindo a governação, cultura, a ética e a estratégia. Dando enfâse ao nível das competências profissionais, a adequação e o impacto dos factores motivacionais, é considerado fundamental o evitar de uma cultura de culpabilização e a existência de uma relação e interligação entre os objectivos pessoais e os objectivos estratégicos organizacionais.

Por seu lado, Samad-Khan (2004) identifica como vantagens de um eficiente programa de gestão do risco operacional, a contribuição para a redução das perdas, uma diminuição dos custos de resolução dos impactos, o aumento da satisfação dos clientes e dos colaboradores, desse modo melhorando a performance da instituição e promovendo a criação de valor para os accionistas.

Moody´s (2004) afirma que o que o capital é parte integrante e importante para enfrentar o risco operacional, no entanto, este é apenas uma das defesas contra o risco e é improvável que seja a única solução e a preferida. O aumento do capital regulamentar não irá por si só reduzir a exposição aos riscos, poderá inclusivamente impactar negativamente ao nível da competitividade da instituição, como consequência do aprovisionamento e da retenção de capital adicional (Chouchy et al., 2003).

De igual modo, o Comité de Basileia (BCBS, 2014) reconhece que o capital não é um substituto de controlos efectivos e do processo de gestão de riscos, pelo contrário, uma forte e efectiva gestão de riscos e um processo alicerçado num ambiente de controlo adequado, ajuda a reduzir as necessidades de capital que as instituições necessitam de alocar para precaver o risco operacional. A gestão de riscos requer experiência, perícia em gestão, sendo requisitos essenciais, envolvendo uma combinação de lógica, de conhecimento tácito (aquele que o indivíduo adquiriu ao longo da vida pela experiência), de previsão. Uma efectiva gestão do risco operacional continuará a ser impulsionada por elementos qualitativos, como uma governação sólida, uma cultura e uma gestão de riscos global que abranja todos os níveis da organização, procedimentos e controlos eficazes, assim como, não de somenos importância, pessoas qualificadas e honestas.

A gestão de risco operacional, segundo Moody´s (2004), melhora a qualidade e estabilidade dos rendimentos, desse modo, permite o reforço da competitividade da instituição financeira, facilitando a sua sobrevivência a longo prazo, pode ser um diferenciador e uma fonte de vantagem competitiva, envolvendo um processo de vigilância constante e de melhoria continua. Abarca a identificação, a análise, o reporte e a monitorização dos riscos operacionais com o objectivo de: (i) identificar oportunidades de melhoria nos processos de negócio; (ii) disponibilizar informação de suporte na tomada de decisões estratégicas; (iii) reduzir os eventos "surpresa" e os respectivos custos operacionais; (iv) identificar e gerir riscos múltiplos, apresentando respostas integradas aos diferentes níveis de risco; (v) transformar os riscos em oportunidades.

Seguidamente, apresenta-se a finalidade da gestão de riscos de acordo com COSO (2007):

- Alinhar o apetite ao risco com a estratégia da organização, definindo os objectivos a elas relacionados e desenvolvendo mecanismos para gerir esses riscos;

- Fortalecer as decisões em resposta aos riscos, possibilitando o rigor na identificação e na selecção de alternativas de respostas aos riscos - como evitar, reduzir, compartilhar e aceitar os riscos;

- Aproveitar as oportunidades, ao capturar eventos potenciais a organização posiciona-se para identificar e aproveitar as oportunidades de forma proactiva;

- Optimizar o capital possibilita a condução de uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

Para Kennett (2003), criar o ambiente adequado e uma cultura apropriada é um dos objectivos de uma boa gestão de riscos, a qual deve fazer parte e estar embutida na cultura da instituição. Todas as decisões e acções, independente da sua magnitude, desde decisões críticas, até às decisões tomadas no dia-a-dia, devem precaver e prever o risco operacional envolvido. Só desta forma, será possível converter este processo num automatismo subconsciente e enraizado nas acções correntes da instituição. De acordo com Samad-Khan (2004), uma gestão de risco operacional, que tente avaliar todos os riscos dos seus processos e de implementar as respectivas medidas de mitigação, poderá ser contraproducente, uma vez que poderá levar a instituição a intensificar os controlos em áreas

que já exista um excesso de controlo, podendo não intensificar os mesmos noutras áreas mais vulneráveis ao risco operacional, o que representará um completo desperdício de recursos.

Blunden e Thirlwell (2010) reconhecem que grande parte dos eventos de risco operacional são resultado de falhas de pessoas, seja a nível da gestão de topo, da gestão intermédia ou a nível administrativo/operações. No entanto, para as organizações esta gestão de riscos associados às pessoas, tem um peso relativo e não é considerado como um elemento chave para a gestão global dos riscos a que a organização está exposta.

Por conseguinte, Hoffman (2002) defende que uma das razões para que a gestão do risco operacional tenha saído da obscuridade deveu-se ao facto de uma parte significativa do risco operacional estar associado ao comportamento humano. Deste modo, para tornar efectiva a gestão do risco operacional será necessário obter uma rede de contactos entre as diversas áreas da organização, devendo existir pontos de contacto nas diversas direcções por forma a estender e propagar a gestão do risco operacional, com a abrangência requerida e expectável. Este espírito colaborativo terá como resultado final uma cooperação entre as diversas equipas, assegurando a correcta percepção dos riscos operacionais a que a instituição está exposta (Kennett, 2003).

Tendo presente esta filosofia de gestão do risco operacional, Hubner, Laycock e Peemoller (2003), identificam um visão menos reactiva, e mais proactiva da gestão deste risco. Passando duma imagem em que os eventos "passam pela instituição", faz-se a gestão da crise e revê-se o processo, para uma gestão proactiva que vá ao encontro dos objectivos da gestão do risco operacional (Figura 2.5).

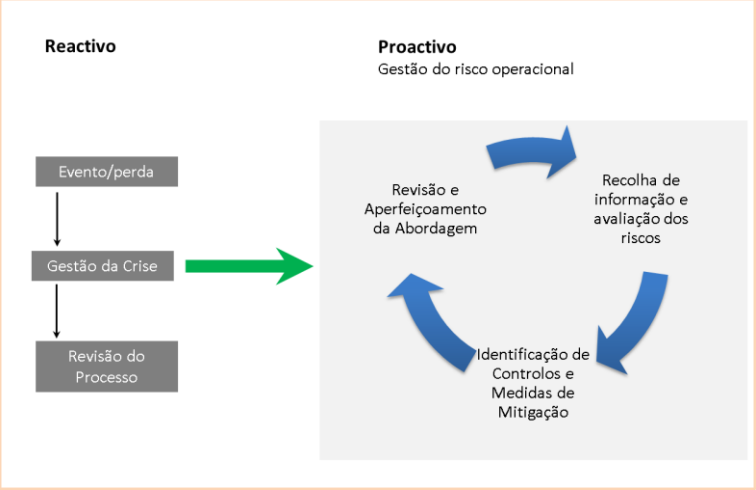

Figura 2.5 – Estilos de Gestão de Risco Operacional

(Fonte: Hubner, Laycock & Peemoller, 2003)

De acordo com Brink (2002), a percepção é o factor mais importante no controlo do risco operacional, os gestores de topo devem estar cientes das consequências, mas também das causas do risco operacional, e que estas advêm não só das áreas operacionais das instituições. O risco operacional existirá sempre onde pessoas, sistemas e processos estão presentes, ou na exposição a eventos externos. Não existindo, ou sendo muito difícil a identificação de áreas onde o risco operacional não está presente.

Em consonância com os pontos referidos anteriormente, Samad-Khan (2004), indica que o objectivo de um sistema de gestão de risco operacional conceptualmente moderno, deve providenciar informações fidedigna aos gestores, por forma a que estes tenham a percepção dos riscos mais significativos a que a instituição está exposta e sobre a adequação dos controlos internos, o que permitirá comportamentos e a tomada de decisões fundamentadas, aquando do desenvolvimento da gestão e da mitigação dos riscos e da estratégia de transferência dos mesmos. Por seu lado, Metchian (2003) entende e enfatiza que o fundamental é que essa gestão do risco aumente o sucesso do negócio e permita a criação de valor, e não apenas o foco no cumprimento dos regulamentos e nos requisitos de capital.

Uma dificuldade reconhecida por Kalhoff e Haas (2004) deriva do facto do conhecimento humano ser criado pelas experiências pessoais directas ou indirectas. Como consequência, existem alguns aspectos de natureza humana que poderão alterar o alcance da identificação e recolha de fragilidades, com impacto na criação de uma base de dados de perdas com qualidade, que permita ao longo do tempo alicerçar e servir de base confiável para a medição e o controlo dos riscos operacionais nas instituições financeiras. Por conseguinte, um dos factores críticos de sucesso para a gestão do risco operacional é a boa vontade e a complacência dos colaboradores na recolha de dados e informação relevante, motivados positivamente ou negativamente por sistemas de incentivos. A tendência para ocultação de erros, de comportamentos inadequados e o actual mercado de trabalho, contribuem para a não comunicação de eventos e influenciam negativamente a cultura de risco da instituição. Os colaboradores têm um papel importante a desempenhar na gestão e na mitigação do risco operacional das instituições e devem estar cientes das suas responsabilidades no que diz respeito à identificação, gestão, monitorização e reporte de risco operacional. Uma forte cultura de risco, que atravesse toda a organização deve ser pré-requisito, não devendo existir a cultura da culpabilização, por forma, a permitir assumir o erro ao contrário de escondê-lo. Tal cultura só é possível alcançar com o apoio directo e activo do órgão de administração (EBA, 2014).

Metchian (2003) entende que as instituições que são boas a gerir o seu risco operacional, criam um sistema que maximiza e procura a contribuição das pessoas. Os objectivos de risco operacional são considerados como outros objectivos de negócio, fazendo parte da cultura e responsabilizado a gestão corrente da instituição, como responsáveis pela gestão do risco operacional.

De acordo com o exposto, Marshall (2001) afirma que a abordagem à gestão do risco deve estar de acordo com factores de risco e no que diz respeito aos comportamentos individuais, em particular à competência, à honestidade e à motivação, devendo a gestão do risco abordar os aspectos de melhoria da qualidade dos recursos humanos, através da selecção, da melhoria dos incentivos, da detecção de fraudes, rotação de turnos, gozo de férias obrigatório, controlos e alertas de sistemas para detecção de comportamentos incorrectos ou arriscados. Por outro lado é dado enfâse aos factores culturais, abarcando a cultura organizacional, a liderança, a comunicação e a moral. A abordagem à gestão de riscos deve nestes casos, alinhar a cultura da gestão com os incentivos, auditorias, políticas, efectuar alterações na liderança e na formação dos recursos humanos, proceder a reestruturações dos postos de trabalho e nas funções, e utilizar ferramentas e processos de comunicação.

Para Blunden e Thirlwell (2010), a cultura é uma função do comportamento individual, relacionado com valores e que é influenciado num ambiente familiar pelas pessoas que o rodeiam. Num contexto de trabalho, o comportamento é influenciado pelos colegas de trabalho e pelas efectivas práticas de negócios (Influência de clientes, concorrência e accionistas). As boas práticas instituídas pelos valores e comportamentos, são efectivas e reais quando postas em prática mesmo quando o indivíduo não está a ser observado, levando a boas decisões criando valor e trazendo vantagens competitivas para a instituição, espelhando uma cultura organizacional saudável, sendo esta a razão e o benefício esperado da gestão de riscos.

3. METODOLOGIA

Ao longo deste capítulo é caracterizada a instituição financeira objecto de estudo e são definidos os procedimentos, metodologia e processo de investigação de recolha e análise de dados adequados à realização da investigação.

Tendo presente a questão, os objectivos e objecto da investigação, a dimensão, tempo e os recursos disponíveis para alcançar os mesmos (Saunders, Lewis & Thornhill, 2009), a estratégia de investigação designada é o estudo de caso. Sendo definido por Robson (2011), como a estratégia de pesquisa que envolve uma investigação empírica de um fenómeno particular contemporâneo, no seu contexto real, baseada em trabalho de campo ou análise documental. Apresentando como característica mais marcante o facto de residir na delimitação do objecto de estudo (Merriam, 1998). Para Yin (2009), o estudo de caso é utilizado em diversas situações para contribuir para o nosso conhecimento sobre o indivíduo, grupo, organização, políticas e fenómenos relacionados. O método de investigação de estudo de caso decorre da necessidade e desejo de compreender fenómenos sociais complexos, podendo ser suportados por dados qualitativos ou quantitativos.

Para Saunders et al. (2009), o estudo de caso permite obter respostas a questões do tipo “Porquê”, bem como a questões do tipo "O quê?" e "Como?". Yin (2009) corrobora que a grande vantagem desta metodologia é quando se colocam questões de “Porquê” e “Como” sobre um conjunto de eventos contemporâneos, ou sobre os quais o investigador tem pouco ou nenhum controlo sobre os eventos. Decorrente das necessidades identificadas e por forma a abranger um maior número de respostas possíveis, a técnica de recolha de dados optada foi a elaboração de um questionário.

Por forma a melhor se compreender o contexto da investigação importa conhecer e caracterizar a instituição financeira. A instituição financeira[5] tem como objecto social o exercício da actividade bancária, fazendo parte de um grupo financeiro que é composto por diversas sociedades especializadas no sector financeiro, nomeadamente no sector bancário e segurador e com presença nacional e internacional. O banco é cotado em bolsa, fazendo parte do índice PSI20 da *Euronext* Lisboa.

A instituição reconhece a gestão dos riscos como sendo um pilar fundamental para garantir a sustentabilidade da mesma, dando ênfase ao foco no equilíbrio entre o risco e o retorno, bem como na redução de efeitos potenciais que possam influenciar ou ter impactos adversos na performance financeira.

Na sequência do referido anteriormente, como método de excelência para a recolha de dados, reitera-se a mais-valia da elaboração de um questionário, face à necessidade de alcançar o maior número de inquiridos possível e da dificuldade acrescida de captar a sua colaboração dada a dimensão da instituição, número de colaboradores e sua dispersão a nível geográfico, sendo impraticável conseguir este desiderato em tempo útil para a conclusão deste trabalho, conceber uma estratégia de recolha de dados através de outros métodos.

O inquérito decorreu durante um período de duas semanas, tendo sido a participação e colaboração solicitada através de correio electrónico institucional a todos os colaboradores, com a indicação da

[5] Relatório de disciplina de mercado da instituição e Relatório de gestão e contas

importância do estudo desenvolvido, bem como, a mais-valia da construção de conhecimento obtido pela participação, garantiu-se ainda o anonimato e consequentemente a confidencialidade das respostas. Deste modo, pretendeu-se objectividade e rigor, sendo possível obter imparcialidade na análise e a recolha de informação relevante. A população que serviu de base para o estudo, teve como universo 1654 colaboradores inquiridos, tendo sido recolhidas 928 respostas ao questionário, o que representa um total de participação de 56% (Figura 3.1).

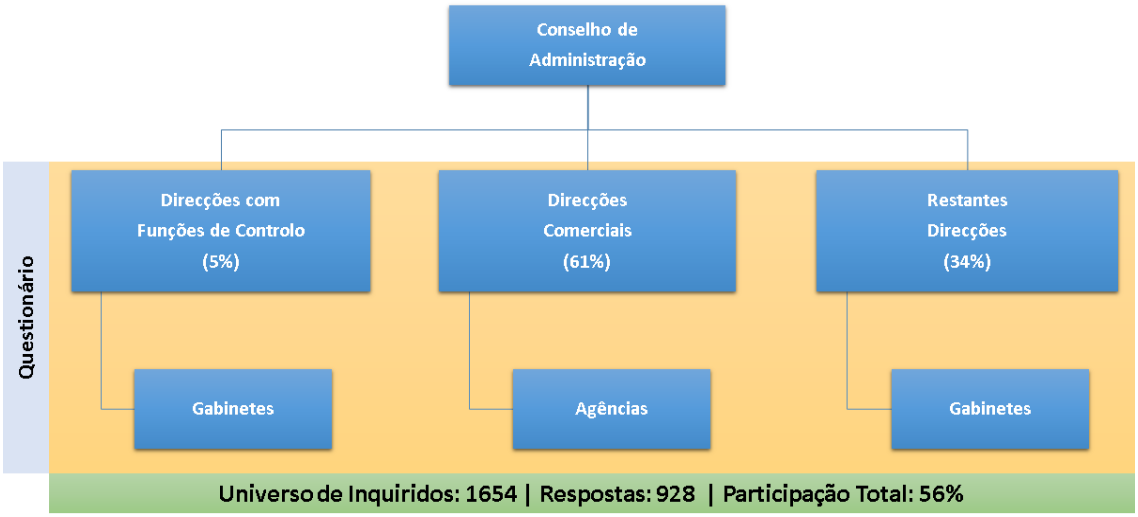

Figura 3.1 - Estrutura hierárquica simplificada da instituição

(Fonte: Elaboração própria)

O questionário teve como suporte uma aplicação interna nativa, específica para realização de inquéritos, permitindo à partida efectuar validações e parametrizações próprias de acordo com o pretendido, bem como, acesso e ligação à base de dados dos colaboradores da Instituição, permitindo a recolha de informação adicional sem a sua intervenção, tornando a resposta ao questionário fluida e sem a geração adicional de erros. Optou-se pela apresentação de questões fechadas por forma a permitir a comparação das respostas pelos diversos grupos internos, facilitar análise estatística, facilitar o preenchimento do inquérito e não obter respostas irrelevantes ou redundantes (Cohen, Manion & Morrison, 2007).

O questionário foi estruturado em três partes distintas, por forma a apresentar a informação de forma natural, coerente, ordenada e que a organização das questões apresenta-se um percurso lógico:

1. **Conhecer o colaborador** – Compreendeu 7 variáveis e 2 questões nas quais se pretendeu caracterizar o colaborador e conhecer a sua experiência profissional. Para as variáveis, não foi necessária a intervenção do colaborador, dada a possibilidade de obter a informação de forma automática, sendo estas a: idade, género, antiguidade na Instituição, antiguidade em Instituições Financeiras, local de trabalho, função interna e

Direcção/Unidade orgânica. Para a questão sobre habilitações literárias, apesar de disponível em sistema, optou-se pela resposta directa do colaborador, uma vez que a mesma poderia estar desactualizada nos registos internos da Instituição.

2. **Conhecer determinados aspectos específicos da cultura da organizacional** – Compreendeu 6 questões com o intuito de aferir atitudes e comportamentos dos inquiridos perante situações que os colocaria em vantagem competitiva perante os seus pares, sobre a partilha e transferência de conhecimento. As questões foram colocadas de modo a avaliar a sensibilidade de cada colaborador, não se pretendendo a resposta certa de acordo com as normas, procedimento e políticas internas.

3. **Testar conhecimentos de risco e particularmente sobre risco operacional** – Compreendeu 17 questões, através das quais se procurou verificar a percepção, comportamentos e o conhecimento sobre a temática do risco operacional, tanto a nível de conceitos básicos, como de questões específicas e de enquadramento na própria Instituição. Pretendeu-se de igual modo, verificar se os colaboradores têm efectiva percepção da estratégia e do processo de gestão de risco operacional definido pela instituição, designadamente no que diz respeito à sua metodologia, ao reporte de eventos e ao papel desempenhado pelos gestores de risco operacional.

Globalmente, a elaboração do questionário foi parametrizado tendo em conta a abrangência do público-alvo (saunders et al., 2009): utilização de linguagem acessível; não complexa; questões curtas e focalizadas no objectivo; não ambíguas, por forma a não obter diferentes interpretações; sem a utilização massiva de termos e questões técnicas, para que o colaborador não despendesse demasiado tempo a compreender a questão e a responder ao questionário.

A elaboração das questões presentes no questionário, basearam-se em diversos elementos informativos e de apoio, os quais espelham e reflectem a cultura da instituição e em particular a cultura de gestão de riscos, na Missão, na Visão e nos Valores da Organização, em documentos públicos, dos quais se destacam, o Relatório de Disciplina de Mercado, o Relatório de Gestão e Contas, o Código de Conduta, em Regulamentos e na Política da Qualidade.

A formulação das questões e a respectiva sequência teve como base quatro passos básicos (Foddy, 1993), os quais são considerados essenciais para que seja bem sucedida a interacção do inquirido com o inquérito, da forma e com a intenção requerida pelo investigador, a Figura 3.2, apresenta a esquematização do processo que consistem em diversas etapas que permitiram aferir e garantir a validade e fiabilidade das questões.

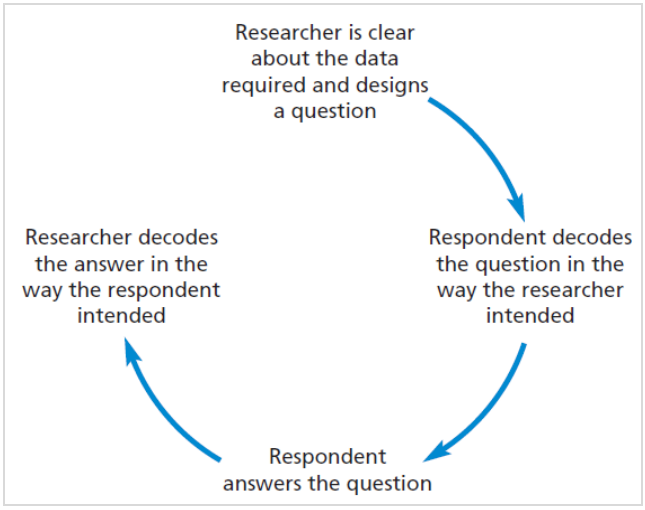

Figura 3.2 – Etapas de validação

(Fonte: Saunders et al., 2009)

Através da utilização dos recursos disponibilizados pela instituição pretendeu-se garantir visibilidade ao inquérito, uma participação significativa, a disponibilidade e empenhamento dos inquiridos perante a solicitação de colaboração, a obtenção de respostas válidas e que reflectissem a realidade do seu ambiente natural.

4. RESULTADOS E DISCUSSÃO

Neste capítulo, são apresentados os resultados da análise efectuada de acordo com a metodologia identifica na dissertação. Tal como referido anteriormente, as respostas ao questionário foram do tipo fechadas por forma a permitir a comparação estatística objectiva dos resultados (Saundres et al., 2009), facilitar o tratamento e análise da informação. Foram colocadas questões que permitissem recolher três tipos de variáveis: (i) opinião, representam o que os inquiridos sentem sobre a questão e julgam ser verdade ou falso; (ii) comportamento, representam uma experiência concreta, o que os inquiridos fazem e o que são. Contem informação sobre o que fizeram no passado, fazem ou irão fazer; (iii) atributo, representam uma experiência concreta, o que os inquiridos fazem e o que são. Contem informação sobre as características dos inquiridos, incluindo características de idade, género, habilitações, ocupação, entre outros.

4.1. ABORDAGEM AO RISCO OPERACIONAL

Compete ao Conselho de Administração da instituição a definição de politicas e estratégias de gestão de riscos, bem como, promover a revisão periódica das políticas e procedimento instituídos, por forma a reflectir as alterações na regulamentação, nos mercados, nos produtos e nas melhores práticas.

Ao nível da estrutura organizacional, a gestão de riscos é assegurada através de três linhas de defesa.

1.ª Linha de defesa: Direcções de Negócio

Gerem o risco associado às suas actividades de acordo com regras e limites pré-definidos presentes na estratégia, políticas e manuais internos.

2.ª Linha de Defesa: Funções de Controlo Independentes - Gestão de Riscos e *Compliance*.

Unidades responsáveis pelas actividades que asseguram o controlo dos riscos, a qualidade dos dados nos sistemas de informação que constituem *input* para os sistemas de informação de risco, a monitorização e avaliação de performance, bem como o controlo do risco global (por exemplo: identificação, medição, limite e mitigação).

3.ª Linha de Defesa: Auditoria Interna

Responsável pelas revisões independentes, monitorização e teste da conformidade com as políticas de risco e procedimentos, assegurando a avaliação regular da efectividade da estrutura de gestão de risco.

Por outro lado, consciente da importância de uma monitorização e controlo eficaz do risco operacional a instituição adoptou uma estratégia de controlo sistemático das áreas que representam risco operacional, desenvolvendo um modelo de gestão cujos principais objectivos são o conhecimento de forma aprofundada dos riscos operacionais incorridos e o desenvolvimento de planos de acção para a sua mitigação.

De modo a alcançar os objectivos propostos foram designados Gestores de Risco Operacional para as diversas áreas da instituição. O perfil de gestor de risco operacional contempla um forte domínio dos temas da sua área de intervenção, designadamente, ao nível do conhecimento dos processos de

negócio, e capacidade de sugestão de medidas de mitigação, assegurando o registo e acompanhamento em aplicação específica para a gestão do risco operacional, de todos os eventos que possam originar perdas financeiras.

A instituição procede à identificação, medição, monitorização, controlo e mitigação dos riscos operacionais em todas as áreas de actividade, classificando-os conforme as tipologias de risco e os segmentos de actividade definidos no Regulamento (EU) N.º 575/2013 do Parlamento Europeu e do Conselho. O modelo de gestão adoptado permite capturar e organizar a informação ao longo das seguintes fases: Recolha, Mitigação, Monitorização e Reporte. A instituição financeira utiliza o Método do Indicador Básico para o cálculo de requisitos de fundos próprios para risco operacional.

4.2. CONHECER O COLABORADOR/POPULAÇÃO

Neste ponto são caracterizados e apresentados os atributos dos inquiridos, agrupando-se por dois grandes grupos, o primeiro macro grupo é composto por direcções: Direcções comerciais, Direcções com funções de controlo e outras Direcções. O segundo macro grupo representa as funções desempenhadas pelos inquiridos: gestão intermédia e sem função de gestão.

O estudo revelou que 65% dos inquiridos são do sexo masculino, 62% têm formação superior e cerca de 1/3 tem até 10 anos de antiguidade em Instituições financeiras (Tabela 4.1).

Habilitações literárias	
Licenciatura	49%
Escolaridade obrigatório	22%
Ensino Secundário	12%
Pós-graduação	10%
Outra	4%
Mestrado	2%
MBA	1%
Doutoramento	0%

Antiguidade em Instituições Financeiras (Anos)	
0-5 Anos	3%
5-10 Anos	32%
10-15 Anos	20%
15-20 Anos	16%
20-25 Anos	15%
> 25-30 Anos	14%

Tabela 4.1 – Habilitações literárias e antiguidade em Instituições Financeiras

Globalmente, 67% dos inquiridos indicam que não tem qualquer formação em risco operacional, sendo que 24% têm formação profissional ou auto-formação. O elevado número de inquiridos sem formação, poderá levar a que os mesmos, perante possíveis eventos, tenham dificuldade em distinguir aqueles que se enquadram neste tipo de risco (Figura 4.1). Nos pontos seguintes será verificada a validade desta suposição, realizando uma análise mais profunda e incisiva, tendo por base a resposta a questões sobre a identificação e o reporte de eventos de risco operacional.

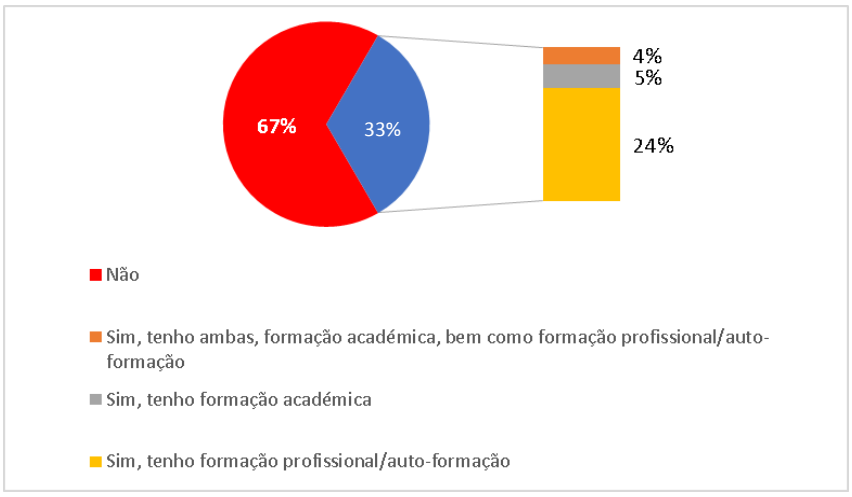

Figura 4.1 – Inquiridos que têm formação em risco operacional

Analisando com maior detalhe as respostas dadas anteriormente, apresenta-se a Figura 4.2, destacando-se pela positiva as direcções com funções de controlo, em que 56% indicam que possuem algum tipo de formação em risco operacional.

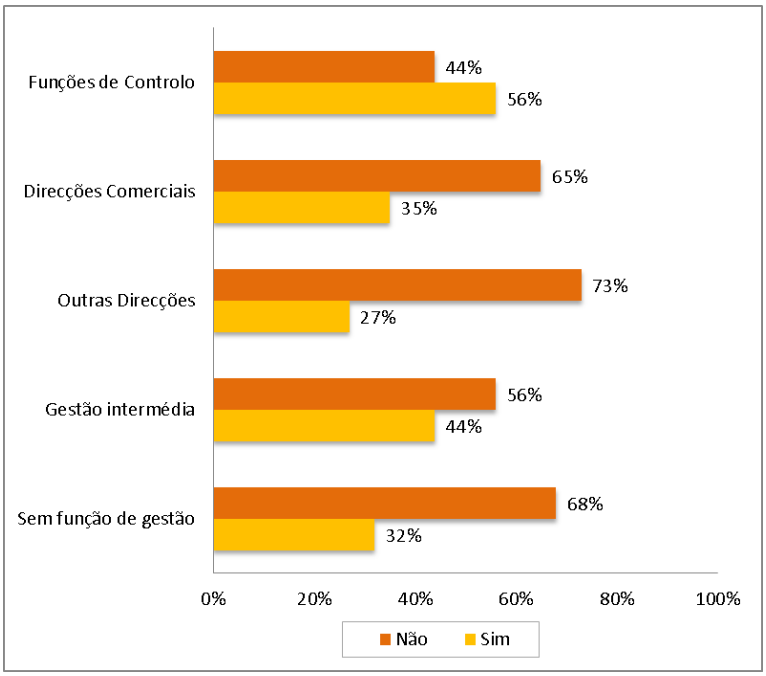

Figura 4.2 – Formação em risco operacional | Detalhe por Grupos de análise

Por outro lado, destaca-se pela negativa a elevada percentagem de inquiridos que não têm formação em risco operacional, tanto ao nível de direcções comerciais como em direcções de operações, de sistemas de informação e de provedoria (incluídas na designação de "Outras Direcções"), as quais podem contribuir positivamente para a detecção e identificação de eventuais eventos de risco

operacional potenciais e de *near-miss*. No mesmo sentido, salientam-se os 65% de inquiridos das direcções comerciais. Em termos de resultados por função, tanto os que desempenham funções de gestão intermédia como os restantes inquiridos, uma grande percentagem indica que não têm formação em risco operacional, com maior preponderância para os inquiridos sem função de gestão.

4.3. CONHECER DETERMINADOS ASPECTOS ESPECÍFICOS DA CULTURA DA ORGANIZAÇÃO

Ao longo do capítulo serão apresentados comportamentos e atitudes dos inquiridos perante diferentes situações das quais é expectável que tenham presente as normas, o código de conduta e a cultura de integridade vigente na instituição, entre as quais a integridade pessoal, relacional e institucional. A integridade "deve pautar a atitude de todos os Colaboradores no desempenho diário das suas funções, com elevados padrões de ética e competência, reflectindo a sua formação como pessoas, como profissionais e como cidadãos". "Os Clientes devem ser colocados em primeiro lugar e usufruir de um serviço de excelência." A referida cultura de integridade deve também reflectir-se na reputação da organização, "enquanto Grupo Financeiro de referência, privilegiando os interesses de médio e longo prazo da nossa Organização e, assim, criando valor para os Accionistas e para as Comunidades onde se inserem as empresas que integram a Instituição."

A Tabela 4.2 apresenta a comparação entre a atitude do inquirido perante o acesso privilegiado ou conhecimento adicional relativo a um processo da instituição, o qual poderia obter uma vantagem competitiva caso não partilha-se esse conhecimento, e a atitude que o inquirido entende que um seu colega teria perante a mesma situação. Pretende-se avaliar a cultura e a disponibilidade de partilha de conhecimento na instituição.

	Opção escolhida pelo inquirido	Opção que o inquirido pensa que o colega optaria
Partilha esse conhecimento com os colegas de equipa	73%	58%
Partilha a informação apenas com os colegas com os quais tenho mais "afinidade"	4%	14%
Comunica apenas ao superior hierárquico	11%	12%
Tendencialmente tenta não obter vantagens para mim próprio	12%	10%
Não partilha a informação, por forma a manter a vantagem competitiva	0%	6%

Tabela 4.2 – Atitude do inquirido perante o acesso privilegiado a um processo da instituição e que o coloca em vantagem competitiva perante os restantes colegas

Verifica-se que a grande maioria dos inquiridos (73%) tende a partilhar o conhecimento com os elementos da mesma equipa, e que os mesmos entendem os seus colegas têm a mesma atitude perante situações análogas (58%). Poderá demonstrar um efectivo alinhamento e partilha de esforços para uma mesma causa. Por outro lado, o acesso à vantagem competitiva poderá ficar confinado a um número restrito de colaboradores, impedindo a instituição de na sua globalidade de

obter a mais-valia deste conhecimento, reflexo da percentagem obtida pela comunicação ao superior hierárquico. No entanto, não é possível afirmá-lo com total certeza, uma vez que por limitação das opções disponíveis aos inquiridos, não era permitida escolha múltipla.

Pelo contrário, perante a detecção de uma falha de controlo num sistema, a grande maioria dos inquiridos considera as opções mais adequadas a comunicação ao superior hierárquico ou a colocação de ocorrência em *helpdesk* (Tabela 4.3). No entanto, observa-se que nas direcções comerciais, a colocação de ocorrência em *helpdesk* tem preponderância sobre a comunicação ao superior hierárquico. Considera-se que esta situação a situação mais correcta, ou prioritária por forma a mitigar com celeridade a falha detectada.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Coloco uma ocorrência no HelpDesk	35%	58%	35%	46%	50%
Comunico ao meu superior hierárquico	58%	36%	59%	48%	44%
Não partilho a informação	0%	1%	0%	0%	0%
Partilho a informação com os colegas com os quais tenho mais "afinidade"	0%	0%	0%	0%	0%
Partilho esse conhecimento com os meus colegas de equipa	7%	5%	6%	6%	6%

Tabela 4.3 - Atitude do inquirido perante o conhecimento de falha de controlo num sistema da instituição

Quando questionados sobre a eventual necessidade de para atingir os objectivos propostos, por vezes ser necessário tomar decisões que poderão ir para além dos riscos que a instituição está disposta a tolerar, pelo menos 65% indicaram que não concordam com a afirmação, independentemente do grupo de análise em que se inserem os inquiridos (Tabela 4.4).

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	11%	17%	13%	21%	14%
Não concordo nem discordo	23%	15%	20%	11%	18%
Discordo totalmente	66%	68%	67%	68%	68%

Tabela 4.4 - Para atingir os objectivos propostos, por vezes é necessário tomar decisões que poderão, eventualmente, ir para além dos riscos que a instituição está disposta a tolerar

Análise que compara com os resultados obtidos relativamente à questão sobre o desenvolvimento regular do negócio, em que mais de 84% das respostas indicam que têm sempre presente as normas, as políticas em vigor, assim como os objectivos da instituição (Tabela 4.5).

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
As normas e políticas em vigor	49%	55%	43%	43%	54%
Os interesses do Cliente	0%	1%	2%	2%	1%
Os meus interesses pessoais	0%	0%	0%	0%	0%
Os objectivos da Instituição	35%	36%	44%	44%	36%
Os objectivos que me foram fixados	16%	8%	11%	11%	9%

Tabela 4.5 - No desenvolvimento da minha actividade tenho sempre presente

De igual modo, verifica-se que a visão estratégica de tolerância e assunção ao risco, em reflexo das normas, políticas e orientações exaradas, "tendentes à execução da prudente estratégia de risco e a evolução da apetência ao risco assumida pelo Banco"[6], são uma preocupação constante dos inquiridos. Por último, sobreleva-se que a generalidade dos inquiridos refere que os seus interesses pessoais são compatíveis com os objectivos organizacionais, verificando-se alinhamento entre as partes nestas matérias.

4.4. TESTAR CONHECIMENTOS SOBRE RISCO E PARTICULARMENTE SOBRE RISCO OPERACIONAL

Neste capítulo pretende-se aferir qual o entendimento dos inquiridos sobre risco na sua essência, qual a percepção que o inquirido tem relativamente ao seu impacto na actividade diária dos inquiridos, se é uma dificuldade acrescida ou se é encarado de forma positiva como uma oportunidade de melhoria e uma mais-valia, avaliar de forma incisiva o conhecimento e as dificuldades inerentes ao conceito e à gestão do risco operacional, apreciar a figura do gestor de risco operacional, pretendendo-se para tal, em algumas das questões apresentadas, a selecção de uma resposta correcta.

Da leitura e análise das Tabelas 4.6, 4.7 e 4.8, verifica-se que as direcções com funções de controlo têm plena consciência do conceito de risco e de risco operacional, que o mesmo é inerente e decorre da actividade da instituição e que representa uma oportunidade de melhoria. Relativamente aos outros grupos estudados, os inquiridos indicam maioritariamente a definição de risco de acordo com a norma ISO 31000, os resultados demonstram igualmente que estão cientes da importância que tem na actividade da instituição.

[6] Política de adequação da instituição

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
O efeito que a incerteza tem nos objectivos e o facto de o resultado do risco poder ser incontrolável e aleatório	40%	49%	50%	49%	50%
O risco é algo com que as organizações têm que conviver por forma a rentabilizar a sua actividade	56%	42%	44%	49%	41%
Todos os processos têm inevitavelmente risco, o qual é impossível de controlar	4%	9%	6%	2%	9%

Tabela 4.6 – Definição de risco

Todavia, as direcções sem funções de controlo (Tabela 4.7), acreditam que o risco é facilmente controlável quando está identificado. Por um lado, e no que diz respeito aos riscos com baixa severidade e de frequência elevada, esta assunção poderá em parte entender-se como razoável, decorrente da sua natureza. Contudo, para eventos de elevada severidade e baixa frequência ou raros, tais como, desastres naturais, grandes fraudes, ataques terroristas, entre outros, este facto já poderá ser menos real e impactar fortemente na actividade e negócio da instituição. A instituição deve evidenciar que mitigar todos os riscos é porventura, uma tarefa não exequível, dado ser humanamente e institucionalmente impraticável, devido à escassez de recursos monetários, humanos e decorrente do próprio conceito de risco. No entanto, a instituição deve claramente enaltecer que devem ser identificados, implementados controlos eficazes e estar ciente de quais poderão impactar na sua actividade. Releva-se o facto de cerca 12% dos inquiridos das direcções comerciais e daqueles que não desempenham funções de gestão considerarem que a temática do risco lhes dificulta o trabalho, o que representa uma visão negativa do risco.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Uma oportunidade de melhoria	49%	44%	42%	52%	42%
Algo que é facilmente controlável quando identificado	42%	44%	49%	42%	46%
Algo que me dificulta o trabalho	7%	12%	7%	6%	11%
Na minha actividade não existe risco	2%	0%	2%	0%	1%

Tabela 4.7 – Qual a percepção do inquirido relativamente ao risco

No que diz respeito ao conceito de risco operacional (Tabela 4.8), pelo menos 75% dos inquiridos indicaram como definição a que está instituída internamente na instituição o que revela algum conhecimento sobre o tema.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Risco de perdas resultantes de uma inadequação ou deficiência de procedimentos, de recursos humanos, de sistemas ou de acontecimentos externos, incluindo os riscos jurídicos	84%	75%	80%	83%	77%
Probabilidade de ocorrência de eventos que afectem de forma significativa a condição financeira da instituição	2%	9%	7%	10%	8%
Um termo geral que se aplica a todas as falhas que influenciem a volatilidade da estrutura de custos da empresa ou estrutura de proveitos	7%	8%	8%	1%	9%
Todo o risco que não seja risco de crédito ou risco de mercado	7%	6%	4%	6%	5%
Não sei	0%	2%	1%	0%	1%

Tabela 4.8 – Definição de risco operacional

Seguidamente, por forma a avaliar a compreensão sobre a temática do risco operacional e exemplificando com situações práticas, elaborou-se um conjunto de questões retratadas por 5 eventos, sendo que, apenas 3 se enquadram em eventos de risco operacional. Cada alínea possibilitava a escolha entre duas opções: sim é um evento de risco operacional; não é um evento de risco operacional. Na tabela 4.9 apresenta-se apenas a percentagem de respostas correctas para cada alínea. Verifica-se que as funções de controlo identificaram sem dificuldade a perda de crédito. Todos os grupos analisados apresentam alguma dificuldade em diferenciar uma perda relativa a risco de estratégia de um risco operacional (alínea d.), com excepção dos inquiridos com funções de gestão intermédia, pelo facto de pelo menos 71% responderam acertadamente a cada uma das alíneas. Comparando as direcções comerciais com as restantes, observa-se que em média têm maior dificuldade em identificar quais são os eventos de risco operacional.

	Direcções			Funções	
Respostas Correctas (%)	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
a. Perda relativa a risco de crédito	91%	68%	75%	89%	69%
b. Perda relativa a risco operacional	70%	71%	73%	82%	71%
c. Perda relativa a risco de mercado	63%	62%	62%	75%	60%
d. Perda relativa a risco estratégico	56%	53%	58%	71%	52%
e. Perda relativa a risco operacional	77%	74%	77%	80%	74%
f. Perda relativa a risco operacional	86%	85%	91%	86%	87%
Média respostas correctas	74%	69%	73%	81%	69%

Tabela 4.9 – Respostas correctas na identificação de riscos

No que diz respeito à detecção de eventos de risco operacional (Tabela 4.10), destaca-se o facto de 63% dos inquiridos das áreas comerciais indicarem que nunca estiveram perante um evento de risco operacional, ou que não estão familiarizado com a temática. Por outro lado, as direcções com funções de controlo, como expectável, no decurso regular das suas actividades procederem à elaboração de relatórios periódicos, com informação relativa à exposição da instituição a cada uma das categorias de risco subjacentes à actividade desenvolvida, estando o risco operacional sujeito ao referido acompanhamento. Assume-se portanto, que a elevada percentagem de inquiridos que identificaram eventos de risco operacional (74%), esteja relacionado com esta constatação.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Sim	74%	37%	55%	72%	41%
Não	19%	50%	28%	20%	44%
Não sei	5%	7%	5%	4%	6%
Não estou familiarizado com os eventos de Risco Operacional	2%	6%	12%	4%	9%

Tabela 4.10 – Esteve perante, ou detectou algum evento de Risco Operacional

Tendo por base o universo de colaboradores que indicou que já esteve perante algum evento de risco operacional e tendo presente as possíveis opções de resposta (Tabela 4.11), verifica-se que apenas uma minoria reporta os riscos detectados de acordo com os procedimentos definidos na instituição, através da colocação de ocorrência em *helpdesk* e reporte ao gestor de risco operacional, podendo porventura, impactos potenciais relacionados com eventos de risco operacional não serem registados e não obterem tratamento adequado por parte da gestão do risco operacional. Do mesmo modo, poderá impactar no registo adequado do evento na aplicação específica e dedicada ao RO, com o objectivo de alimentar uma base de dados de risco operacional fiável, abrangente e que contribua para o aumento da sua robustez, para que espelhe o perfil e a real exposição ao risco operacional da instituição (Goncalves, 2011).

Verifica-se que nas direcções com funções de controlo apenas 35%, faz a comunicação ao gestor de risco operacional, pelo contrário, nas direcções comerciais, o peso deste reporte é de 53%. Conclui-se portanto, que se não existir um relacionamento constante e tempestivo, entre as funções de controlo e a área de gestão do risco operacional, os eventos identificados poderão ficar excluídos no que diz respeito à respectiva análise na vertente da gestão do risco operacional.

Na avaliação das respostas por função, tanto os inquiridos com função de gestão intermédia, como os restantes inquiridos, convergem na atitude de reporte ao gestor de risco operacional, 44% e 42% respectivamente, sendo manifestamente inferior ao desejável.

De destacar, que o facto de não se reportar eventos de risco operacional, não está relacionado com o receio de represálias, consequências negativas ou de imputação de responsabilidades. Este resultado evidência um comportamento saudável emanado pela cultura da organização.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Coloquei uma ocorrência no HelpDesk e reportei ao meu Gestor de Risco Operacional	22%	43%	21%	35%	31%
Reportei apenas ao meu superior hierárquico	28%	19%	30%	16%	26%
Avaliei o sucedido e adoptei apenas as medidas de mitigação que considerei necessárias	19%	8%	15%	18%	10%
Outra iniciativa	16%	4%	16%	13%	10%
Reportei apenas ao meu Gestor de Risco Operacional	13%	10%	11%	9%	11%
Coloquei apenas uma ocorrência no HelpDesk	2%	15%	5%	9%	10%
Não reportei por recear represálias, consequências negativas ou que me sejam imputadas responsabilidades	0%	1%	1%	0%	1%
Não reportei porque posso estar a cometer um erro de avaliação	0%	0%	1%	0%	1%

Tabela 4.11 – Qual a atitude do inquirido perante o evento de risco operacional

Quantificando o número de eventos que o inquirido já reportou, apresenta-se a Figura 4.3, onde se observa que 64% dos inquiridos nas áreas comerciais, nunca reportaram sequer um evento de risco operacional, situação análoga se observa em inquiridos sem funções de gestão (60%). Valores que comparam com os apresentados anteriormente na Tabela 4.10, em que se identificam estes dois grupos, como sendo os que não detectaram nem estão familiarizados com eventos de risco operacional.

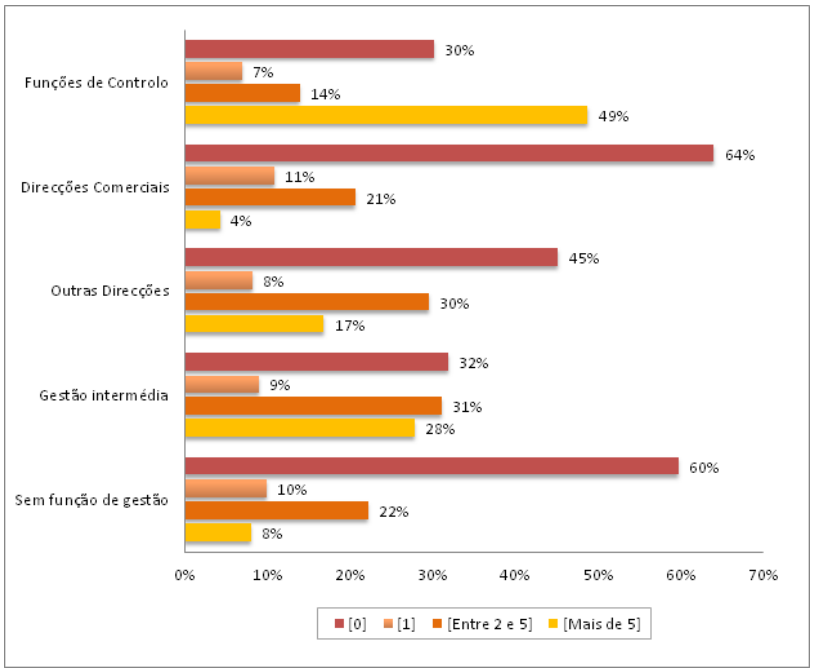

Figura 4.3 – Nº de Eventos de Risco Operacional reportados

Dos inquiridos que reportaram zero eventos de risco operacional (Tabela 4.12), verifica-se que uma percentagem relevante (média de 17% na comparação entre direcções e de 22% decorrente da segregação pela função), não reporta eventos, porque avaliam os mesmos e são logo tomadas as medidas de mitigação que se julgam necessárias e suficientes, dando-se também particular destaque aos 33% dos inquiridos que desempenham funções de gestão intermédia. Infere-se que desta atitude poderá tal como indicado anteriormente, ter como consequência a contribuição para não se registar eventos na aplicação própria para o efeito, de não se implementar medidas de mitigação sustentáveis e duradouras, focarem por implementar controlos eficazes, face à implementação de medidas de remediação avulsas e possivelmente restritas a uma determinada actividade ou tarefa e não dirigidas ao processo de uma forma holística. Não sendo possível manter uma base de dados com a qualidade necessária e os registos suficientes para análises futuras consistentes e tendo em vista a evolução no espectro das metodologias disponíveis, bem como, de contribuir para o desenvolvimento de práticas e sistemas de medição de risco operacional mais sofisticados e consequentemente, ter a possibilidade de reduzir os requisitos de fundos próprios para a cobertura do risco operacional, nomeadamente por via da adopção de métodos mais avançados.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Não reportei porque nunca estive perante, nem detectei, qualquer evento de Risco Operacional	62%	79%	62%	56%	75%
Avaliei o sucedido e tomei as medidas de mitigação que considerei necessárias	23%	10%	17%	33%	10%
Não sei quando estou perante um evento de Risco Operacional	0%	4%	14%	3%	7%
Outra iniciativa	7%	0%	2%	0%	2%
Não reportei porque posso estar a cometer um erro de avaliação	0%	6%	4%	8%	5%
Não reportei por recear represálias, consequências negativas ou me sejam imputadas responsabilidades	8%	1%	1%	0%	1%

Tabela 4.12 – Motivo pelo qual nunca reportou eventos de Risco Operacional

Posteriormente, submeteu-se à apreciação dos inquiridos que já reportaram eventos de risco operacional, sobre o desempenho e eficácia do gestor de risco operacional no acompanhamento deste processo (Tabela 4.13). Em termos médios verifica-se que os inquiridos avaliam o GRO com alguma indiferença e negatividade. Agrupando estas duas apreciações, verifica-se que o grupo representado pelas outras direcções, apresenta 57% de opiniões menos positivas, bem como os inquiridos com funções de gestão intermédia, com 47%. Por forma a melhorar o desempenho dos gestores de risco operacional, deverão ser definidos critérios claros para sua a nomeação, serem avaliados positivamente de acordo com a sua performance no desempenho desta função e reflectida na sua avaliação individual, a obtenção de reconhecimento e de notoriedade pela identificação de eventos com impactos potenciais relevantes poderá ser considerado um incentivo ao reporte. Os GRO na sua área de influência, deverão pautar-se pelo acompanhamento próximo dos eventos identificados, demonstrando que os mesmos são considerados, prestando os devidos esclarecimento e caso não se tratem de eventos que se enquadrem na categoria de risco operacional, esclarecer o colaborador atempadamente e adequadamente.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	66%	60%	43%	54%	53%
Não concordo nem discordo	31%	33%	48%	35%	40%
Discordo totalmente	3%	7%	9%	11%	7%

Tabela 4.13 – Avaliação positiva da eficácia do acompanhamento realizado pelo GRO

Por forma a ilustrar a visibilidade da função do gestor de risco operacional colocou-se a questão sobre o conhecimento da existência do gestor de risco operacional na sua área ou direcção (Figura

4.4). Optou-se pela agregação das respostas correspondentes a “Não” e “Não sei”, uma vez que em todas as áreas da instituição existe pelo menos um gestor de risco operacional, sendo para o efeito, equivalente o tipo de resposta.

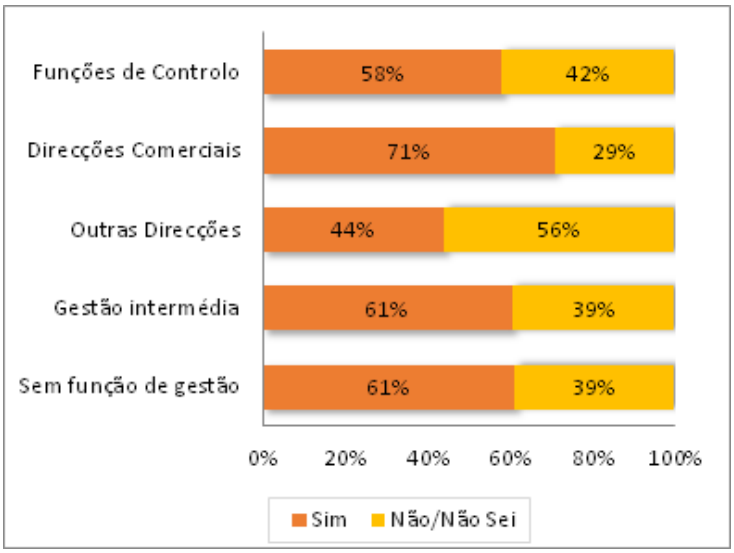

Figura 4.4 – Inquiridos que reconhecem a existência de GRO na sua direcção

No que diz respeito ao macro grupo representativo das direcções, destaca-se pela positiva os 71% de inquiridos das direcções comerciais que indicam ter conhecimento da existência de gestor de risco operacional na sua área, destes, 93% indicam igualmente que sabem exactamente quem é o gestor nomeado (Tabela 4.14). Dos resultados obtidos deduz-se que estes advêm do facto de alguns responsáveis das direcções comerciais, através de correio electrónico, alertarem periodicamente a rede para a importância do risco operacional. Neste aspecto, as direcções comerciais apresentam-se bem informadas.

Pela negativa, salientam-se as direcções com funções de controlo e as outras direcções, com 58% e 44% respectivamente, a identificarem a existência do gestor de risco operacional na sua direcção. Infere-se que o gestor de risco operacional alocado, pode não ser o mais adequado para esta função, uma vez que aparenta estar na obscuridade, que não é habitual trocar e partilhar informações sobre o tema do risco operacional ou que o mesmo não é abordado com frequência.

Aprofundando a análise no grupo de outras direcções, o resultado desta questão apresenta um elevado valor de desconhecimento relativo à função do GRO, nomeadamente por parte de direcções com elevado potencial para identificação e detecção de riscos operacionais, destacando-se a direcção de sistemas de informação, de produtos e de recursos humanos, totalizando em média 74%, esta situação apresenta-se com uma potencial fragilidade. Os gestores de risco operacional alocados a estas direcções, decorrente da sua natureza e da própria definição de risco operacional (Fontes de risco: Processos, Recursos Humanos, Sistemas e Acontecimentos Externos), são um ponto de contacto fundamental entre a respectiva área e para a gestão do risco operacional, contribuindo com sugestões de medidas de mitigação e assegurar o registo e acompanhamento de eventos de risco operacional e participação activa no processo de gestão do risco operacional.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Sei que existe e quem é o Gestor de Risco Operacional que está nomeado para a minha Direcção	72%	93%	88%	95%	90%
Sei que existe mas desconheço quem está nomeado para essa função	28%	7%	12%	5%	10%

Tabela 4.14 – Detalhe | Inquiridos que reconhecem a existência de GRO na sua direcção

É agora importante avaliar o que conduziria os inquiridos a reportar eventos de risco operacional. Para tal, foram apresentadas 6 afirmações, expostas nas Tabelas 4.15 à 4.19 para avaliação dos inquiridos de acordo com a sua sensibilidade ou percepção. Da análise da Tabela 4.15 observa-se que os inquiridos estão predispostos a colaborar no reporte de eventos de risco operacional através de uma aplicação informática dedicada. Esta é uma opinião generalizada entre os grupos estudados, uma vez que mais de 70% concordam com a afirmação. Supõem-se portanto, que a interacção de todos os colaboradores com uma aplicação informática de registo de eventos, permita a recolha de um maior número de eventos de risco operacional e não apenas aqueles a que o gestor de risco operacional tem acesso e conhecimento. Uma possível mais-valia deste processo e ter maior impacto positivo, poderá ser nos 45% de inquiridos que indicaram que nunca estiveram perante, ou detectaram eventos de risco operacional (Tabela 4.10), decorrente do acesso à aplicação e à visualização de outros eventos já reportados, fazerem uma introspecção e uma auto-avaliação sobre se o não reporte de eventos se deveu efectivamente à não detecção dos mesmos ou a falta de consciência para a temática do risco operacional. O acesso generalizado à aplicação possibilita igualmente, a análise de "falsos" eventos de risco operacional reportados, permitindo verificar quais são as maiores dificuldades e quais os erros mais comuns dos colaboradores relativamente à identificação de eventos, podendo-se eventualmente, direccionar futuras acções de formação para estes colaboradores ou sobre os temas que mais dificuldades apresentam. Por outro lado, pode libertar e proporcionar ao gestor de risco operacional o desempenho de um papel mais activo no processo de gestão do risco operacional.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	79%	77%	73%	72%	76%
Não concordo nem discordo	16%	16%	19%	20%	17%
Discordo	5%	7%	8%	8%	7%

Tabela 4.15 - Aceder directamente a uma aplicação informática onde pudesse colocar os eventos de Risco Operacional detectados

De acordo com a Tabela 4.16, observa-se que apenas uma pequena percentagem dos inquiridos, independentemente do grupo de análise, afirmar que a garantia de anonimato como fundamental

para o reporte de eventos, o que compara e corrobora a análise efectuada anteriormente relativamente à predisposição para reportar eventos de risco operacional através de uma aplicação informática, a qual pressupõem a utilização de uma autenticação, não conferindo *à priori* o anonimato no registo de eventos. Verifica-se no entanto, que existe uma elevada taxa de resposta que "Não concorda nem discorda" da afirmação, demostrando indiferença ou quiçá o facto de esta questão não estar à partida a ser equacionada por parte dos inquiridos. Destacam-se também, os 58% de inquiridos com funções de gestão intermédia que discordam com o anonimato, confrontando com 41% dos inquiridos sem funções de gestão. Infere-se que esta diferença poderá decorrer das próprias funções atribuídas à gestão intermédia na participação no processo de avaliação de desempenho dos seus colaboradores. A existência de anonimato comportaria um possível entrave na avaliação e aferição dos colaboradores mais activos e quais os que mais contribuem para o processo de risco operacional. O anonimato representaria um constrangimento relativamente a este ponderador no que concerne à sua utilização a nível de avaliação de desempenho individual.

Decorrente do exposto e analisando de forma agregada os resultados dos inquiridos que concordam e dos que não concordam nem discordam com a afirmação, observa-se que pelo menos 50% dos inquiridos de todos os grupos de análise, com excepção dos que desempenham funções de gestão intermédia, entendem que a garantia de anonimato pode ser um factor determinante no reporte de eventos de risco operacional.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	12%	18%	15%	13%	17%
Não concordo nem discordo	41%	39%	42%	29%	42%
Discordo	47%	43%	43%	58%	41%

Tabela 4.16 - Ter a garantia de anonimato na colocação de eventos de Risco Operacional

Da análise da Tabela 4.17 e à semelhança do descrito na Tabela 4.16, observa-se que existe convergência de opiniões entre os grupos estudados, com excepção do grupo com funções de gestão intermédia. Neste contexto e à luz dos resultados obtidos, entende-se que por parte deste grupo, poderá existir uma cultura de culpabilização, situação que poderá conduzir à ocultação do erro e ao não reporte atempado de incidentes numa fase embrionária e no momento em que são detectados. A ocultação do erro impede a tomada de medidas de mitigação adequadas e eficazes, no tempo certo, por forma a mitigar as fragilidades identificadas, podendo eventualmente, eventos sem impacto material relevantes ou inócuos, degenerar em perdas reais. Por outro lado, entende-se que não se pretenda a total desresponsabilização dos actos dos inquiridos na sua actividade diária, no entanto, no que diz respeito à gestão do risco operacional e na sua essência, pretende-se essencialmente identificar, avaliar, controlar/monitorizar e mitigar os riscos, para tal é necessária a recolha de dados internos de qualidade e não baseados em reportes pobres por se recear a imposição de sanções, tornando este processo ainda mais complexo (Gonçalves, 2011).

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	35%	36%	41%	34%	38%
Não concordo nem discordo	32%	32%	30%	23%	32%
Discordo	33%	32%	29%	43%	30%

Tabela 4.17 - Ter a garantia de que ao reportar eventos de Risco Operacional não iria sofrer represálias, nem consequências negativas ou imputadas responsabilidades pelo reporte

A Tabela 4.18 apresenta os resultados relativos ao reporte de eventos de risco operacional no que diz respeito à sua associação e contribuição positiva para a avaliação dos inquiridos. Verifica-se que nas direcções com funções de controlo e nas outras direcções, existe uma maior percentagem de colaboradores que indicam que concordam com a afirmação, do que aqueles que discordam. Pelo contrário, nas direcções comerciais sucede o oposto. Depreende-se que nas áreas comerciais, pelo facto de existirem objectivos comerciais exigentes, qualificação que decorre do actual contexto económico, a existência de um objectivo adicional a contribuir para a avaliação do colaborador, pode colocar um peso e um esforço adicional na sua actividade diária. Por outro lado, a avaliação do colaborador pode ser direccionada, não para um objectivo adicional, mas para uma forma de reconhecimento pelo bom desempenho na identificação de eventos, de controlos e o contributo para a sua mitigação.

Globalmente, verifica-se alguma indiferença, no que diz respeito ao peso desta variável para o contributo da avaliação dos inquiridos, visto que a opção indicada maioritariamente foi "Não concordo nem discordo", contrariando esta tendência, observa-se que os inquiridos com funções de gestão intermédia, discordam da afirmação.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	40%	23%	33%	27%	27%
Não concordo nem discordo	40%	42%	40%	32%	43%
Discordo	20%	35%	27%	41%	30%

Tabela 4.18 – Reporte de eventos a contribuir positivamente para a minha avaliação

Importa evidenciar que a grande maioria dos inquiridos não tem objectivos que avaliem a sua participação no processo de risco operacional (Figura 4.5), não sendo possível avaliar e valorizar a participação de cada colaborador no processo. Do mesmo modo e decorrente do facto do registo e recolha de eventos ser na sua grande maioria efectuado manualmente, por colaboradores que porventura estiveram envolvidos na sua ocorrência, Goncalves (2011) entende que, caso não existam motivações pessoais para o reporte de fragilidades, existem neste sentido incentivos para as ocultar, tornando a mais complexa a quantificação do risco operacional.

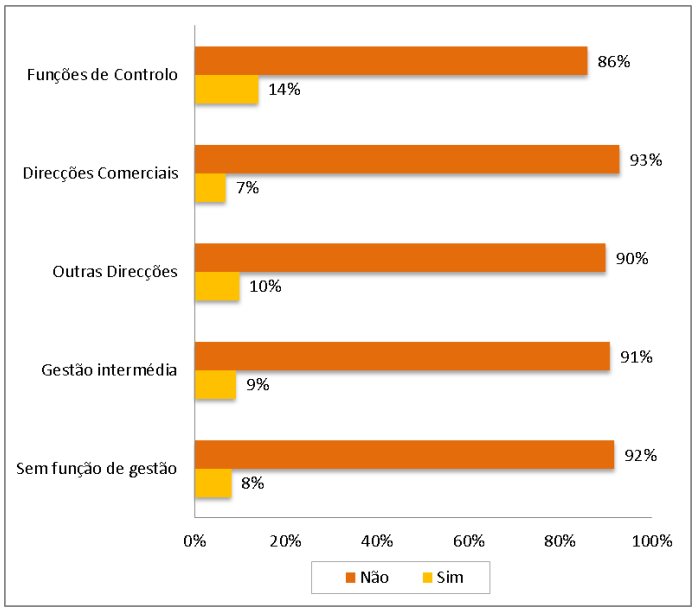

Figura 4.5 – Tem objectivos de risco operacional

De salientar que a quase totalidade dos inquiridos discorda do facto de que o reportar eventos de risco operacional não traz valor acrescentado para a sua função (Tabela 4.19).

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	0%	2%	1%	0%	2%
Não concordo nem discordo	12%	16%	17%	5%	17%
Discordo	88%	82%	82%	95%	81%

Tabela 4.19 - Reportar eventos não traz valor acrescentado para a minha função

No mesmo sentido, verifica-se que é entendido que a gestão do risco operacional não representa um entrave para o desempenho da função dos inquiridos (Tabela 4.20). Demonstrando uma visão positiva da temática do risco operacional.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	2%	1%	1%	0%	1%
Não concordo nem discordo	12%	11%	13%	4%	13%
Discordo	86%	88%	86%	96%	86%

Tabela 4.20 - A gestão de Risco Operacional é um entrave ao desempenho da minha função

Neste contexto, verifica-se que a efectiva e eficaz gestão do risco operacional é percepcionado como sendo gerador de vantagens competitivas para a instituição. Através deste reconhecimento é possível alicerçar e fomentar uma cultura de risco operacional baseada não apenas em pressões regulamentares, de mercado, ou institucionais, mas também através da consciencialização e demostração de que a gestão do risco permite a criação de valor para a instituição e para os colaboradores em todas as suas vertentes. A demonstração das mais-valias da gestão do risco permite a transformação positiva dos comportamentos perante a temática, conduzindo a um reforço da competitividade da instituição, possibilita que seja a fonte de melhoria contínua de processos e de actividades. Deve também ser enfatizada a interligação entre a gestão do risco operacional e o retorno que esta permite, através da valorização do negócio e introdução de melhorias no ambiente de controlo, representando um *trade-off* positivo. É também um investimento recompensado nas abordagens mais avançadas para o cálculo dos requisitos de capital alocado ao risco operacional, sendo uma componente valorizada através do impacto positivo da boa gestão do risco operacional.

Através da análise da Figura 4.6, constata-se que globalmente os inquiridos entendem que a gestão do risco operacional é uma fonte de vantagens competitivas para a instituição, sendo que pelo menos 90% dos inquiridos concordam com as afirmações. É também responsabilidade da própria instituição demonstrar as vantagens que pode trazer ao colaborador, no desempenho da sua função e da sua actividade diária por forma a cimentar e apoiar uma cultura orientada para a identificação dos riscos inerentes às actividade desenvolvidas e encorajados em proactivamente, identificar eventos de risco operacional existentes ou potenciais.

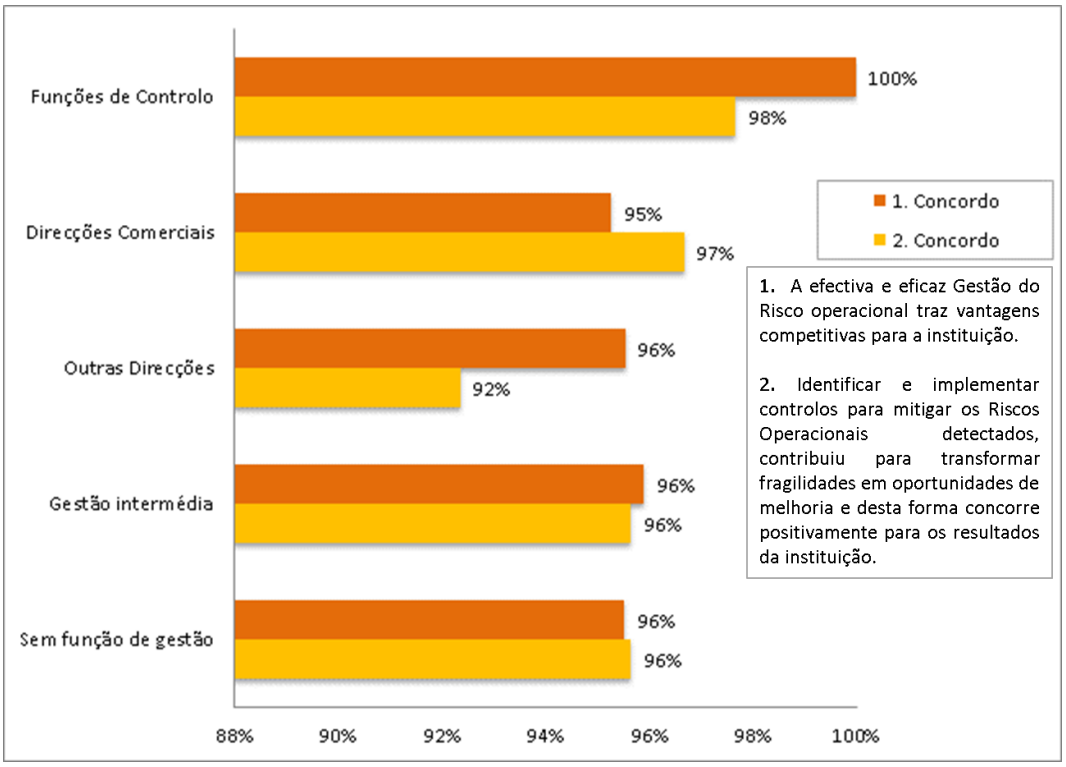

Figura 4.6 – Benefícios da gestão do risco operacional

Na prossecução destes objectivos, e tendo presente as fases do processo de gestão do risco operacional, a identificação, medição, monitorização, controlo e mitigação, refere-se que a identificação e avaliação do risco operacional associados aos produtos, actividades, processos e sistemas não é de somenos importante, principalmente numa fase inicial e no momento em que são criados ou implementados, bem como, a identificação e implementação de controlos chave nesta fase precoce, tornando-se vital para a detecção de fragilidades que possam impactar no desempenho eficiente e rentável da actividade da instituição, garantir a sua competitividade, limitar possíveis impactos materiais e redução dos riscos. Neste sentido, aos inquiridos foi colocada a questão referente ao conhecimento atempado e suficientemente esclarecedor sobre o lançamento de, alteração, ou descontinuação de normativo referente a produtos, serviços ou divulgação de novos processos (Tabela 4.21). Dos inquiridos que concordam com a questão, observa-se que entre as direcções analisadas, as direcções comerciais são as que se consideram mais informadas sobre esta matéria, com 64 %. Por outro lado, as direcções com funções de controlo apresentam 56%, o que no entender do autor, representa um valor pouco positivo, decorrente do papel que estas direcções representam no processo de gestão de riscos e em particular na gestão do risco operacional. A identificação de riscos operacionais deve ocorrer, tal como justificado anteriormente, na fase de implementação, desenvolvimento ou alteração de produtos, processos, actividades e sistemas, permitindo a tomada de decisões fundamentadas sobre a estratégia a seguir perante o risco operacional, tal como, no que diz respeito ao seu controlo e mitigação. Segundo Brink (2002) as opções estratégicas a tomar de acordo com o perfil de risco são: (i) evitar o risco; (ii) mitigar o risco; (iii) transferir o risco; (iv) aceitar o risco. Sublinha-se que as outras direcções apenas 42% concordam com a questão colocada.

Realça-se igualmente, que a divulgação atempada das normas é essencial para a própria gestão do conhecimento interno da instituição, é um factor fundamental no actual contexto de crescente complexidade de produtos, procedimentos e regulamentos, por forma a evitar erros dos colaboradores por desconhecimento ou por falta de tempo para analisar a informação que lhes é disponibilizada e porventura essencial para o desempenho adequado das suas funções. A partilha de responsabilidades pela gestão do risco operacional deve comportar um esforço conjunto e colaborativo, entre a equipa de risco operacional e as restantes áreas da instituição por forma a assegurar que as áreas têm a percepção e conhecimento dos riscos que gerem.

No que diz respeito à segregação de resultados pelas funções que os inquiridos desempenham, observa-se que dos que desempenham funções de gestão intermédia apenas 48% concordam com a questão, contrapondo com 57% dos restantes inquiridos. Depreende-se portanto que, ao nível dos gestores intermédios, de acordo com as responsabilidades inerentes à função e ao conhecimento transversal que detêm dos processos da instituição, pretendem maior celeridade e em tempo oportuno, a obtenção de acesso a informação sobre produtos, serviços e processos, podendo desta forma a analisar com detalhe o conteúdo das normas, no seu âmbito, objectivos, alcance e riscos associados.

	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Concordo	56%	65%	42%	48%	57%
Não concordo nem discordo	26%	18%	37%	26%	25%
Discordo	18%	17%	21%	26%	18%

Tabela 4.21 – Tem conhecimento atempado e suficientemente esclarecedor sobre o lançamento de, alteração, ou descontinuação de normativo referente a produtos, serviços ou divulgação de novos processos

Por fim apresenta-se a percepção que os inquiridos têm sobre o acesso à temática do risco operacional e se entendem que é esclarecedora. Neste contexto apresenta-se a Figura 4.7, onde se observa que a grande maioria dos inquiridos das direcções com funções de controlo e outras direcções, pelo menos 77% identificam que a informação existente não é esclarecedora nem de fácil acesso. Por outro lado, nas direcções comerciais, 57% dos inquiridos indicam que não é de fácil acesso, e 61% afirmam que não é esclarecedora.

No que diz respeito aos inquiridos com funções de gestão intermédia, observa-se que mais de 78% entende que a informação não é de fácil acesso nem esclarecedora, quanto aos inquiridos sem funções de gestão, apresentam valores um pouco mais favoráveis com 63% a indicar que a informação não é de fácil acesso e 68% que não é esclarecedora.

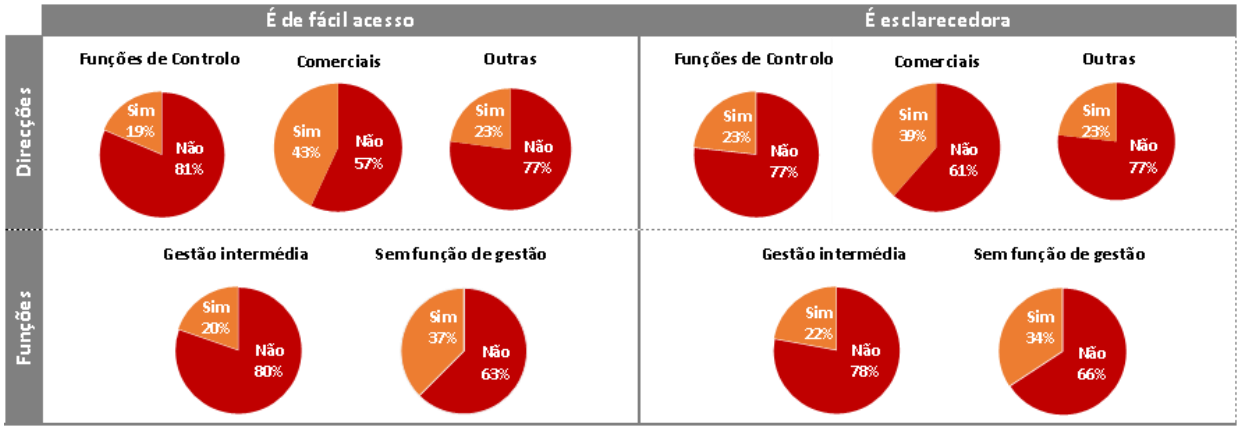

Figura 4.7 – Informação sobre a temática do risco operacional que existe na instituição

Analisando os resultados, entende-se que existe uma lacuna no que diz respeito à gestão de conhecimento e de acesso à informação sobre esta temática, dificultando porventura, a disseminação e incorporação da cultura de risco operacional na instituição. É reconhecido que a implementação de um sistema de gestão do conhecimento (Brick, 2002) é de extrema importância para a adequada mitigação do risco operacional, e em todas as fases do processo do risco operacional.

5. CONCLUSÕES

A consciencialização para o risco operacional é dos factores mais importantes para o seu controlo, por conseguinte deve ser evitada a ideia que o risco operacional é específico de determinadas áreas da instituição. Sendo muito difícil identificar áreas livres de risco operacional, coexistindo com as pessoas, sistemas, processos ou em exposição a riscos externos.

Este estudo pretendeu verificar a efectividade da metodologia vigente de disseminação e incorporação de gestão do risco operacional na cultura da instituição, identificando-se como um conjunto de valores, crenças, atitudes e normas compartilhadas que moldam o comportamento e as expectativas de cada membro da organização (Stoner & Freeman, 1982). Para tal foi necessário aprofundar questões específicas por forma a responder cabalmente ao objectivo apresenta na dissertação. Por conseguinte, serão apresentadas as conclusões para cada um dos objectivos específicos:

Conhecer as dificuldades inerentes à identificação, recolha e análise dos eventos de risco operacional detectadas, por parte dos diferentes níveis hierárquicos estudados – Da análise dos resultados obtidos, verifica-se que os inquiridos sem funções de gestão identificam claramente a definição de risco operacional de acordo com a que está instituída na organização, no entanto, revela-se que existe carência de formação sobre a temática do risco operacional, facto que pode explicar as dificuldades sentidas na identificação de eventos. A generalidade dos inquiridos deste grupo, tem uma visão excessivamente simplificada do risco sendo considerado como facilmente controlável quando está identificado. Contudo, regem-se por elevados padrões de ética, competência e qualidade, decorrente do código de conduta, política da qualidade, política de gestão de riscos e na divulgação da Missão, Visão e Valores da instituição. Apesar das dificuldades sentidas por este grupo, compreendem que a eficaz gestão do risco operacional pode ser gerador de vantagens competitivas e contribuiu para a criação de valor para a instituição, estando igualmente receptivos a participar mais activamente no processo de risco operacional.

No que diz respeito aos inquiridos com funções de gestão intermédia, as opiniões convergem com o grupo anterior, contudo, existem algumas divergências relevantes. Estes conseguem com grande objectividade e demonstrando pouca dificuldade, distinguir eventos de risco operacional de outros riscos, o que contribuiu para a percentagem substancial de inquiridos que já identificaram e reportaram este tipo de eventos. Verifica-se que são avessos ao reporte de eventos de forma anónima, entendem também, que o reporte de eventos possa gerar represálias, consequências negativas para quem reporta ou imputadas responsabilidades pelo reporte. Esta visão poderá espelhar uma "cultura da culpa" de uma parte da estrutura da instituição, podendo ter como consequência a ocultação de deficiências ou fragilidades identificadas e no encobrimento de falhas e de perdas potenciais. Por fim refere-se qua a sua visão do risco não é tão simplista e mais orientada para a seus aspectos positivos.

Avaliar o comportamento das áreas com funções de controlo perante o risco operacional – Verifica-se alguma passividade no contributo para o enriquecimento do processo de risco operacional, para além daquele que é efectuado através dos relatórios realizados no decurso normal das suas funções. Contributo que não é de somenos importância, podendo desempenhar um papel mais dinâmico tanto na identificação de eventos, de controlos, bem como, no contributo activo para a sugestão de

medidas correctivas adequadas, para a mitigação das fragilidades de risco operacional identificadas pelas diferentes estruturas da instituição. Goncalves (2011) identificou a necessidade e tendência crescente para agregar informação das áreas com funções de controlo e a área de risco operacional. Para tal, é imprescindível um processo de gestão risco operacional eficiente e eficaz que permita a elaboração de relatórios com a agregação de informação destas diferentes áreas, em sequência e através da partilha de conhecimentos e do acesso comum a informação sobre processos, actividades, controlos, testes aos controlos, medidas de mitigação para corrigir as fragilidades detectadas e auto-avaliações realizados a cada risco. Do mesmo modo, o sistema de gestão do risco operacional, facilitará e auxiliará na criação de planos de auditoria interna e na alocação de recursos, ao fornecer informação útil sobre os processos da instituição que se encontram mais fragilizados, contribuindo para a resiliência e solidez da instituição e para a valorização e notoriedade da função de gestão do risco operacional. Foi possível verificar que estes inquiridos apesar de serem os que mais formação têm em risco operacional, considera-se que a percentagem apresentada não é tão elevada como seria desejável. Este raciocínio é reflexo dos resultados globais obtidos, não se vislumbrando diferenças significativas em relação aos restantes grupos estudados.

Verificar se existe uma percepção real para o que é e o que representa o risco operacional por parte das áreas comerciais da instituição financeira – Relativamente às áreas comerciais, verifica-se que existe alguma consonância com as respostas dadas pelos inquiridos sem funções de gestão e dificuldades semelhantes. Esta área apresenta o maior número de inquiridos que indica que quando detecta eventos de risco operacional, o faz de acordo com as normas internas. Não obstante é aquela que indica que nunca esteve perante ou detectou um evento de risco operacional, reconhecendo o autor que esta é uma indicação anormal, uma vez que estes colaboradores são dos mais expostos a eventos de risco operacional (decorrente de análise e prospecção da base de dados de perdas de risco operacional da instituição). Infere-se que a percepção do risco operacional pode ser aparente.

Segundo Stoner et al. (1982), uma das barreiras mais comuns à comunicação é a perspectiva e a percepção que cada pessoa tem relativamente a um mesmo facto, decorrente das diferentes experiências, conhecimentos de cada uma e pela circunstância em que ocorre. Para ultrapassar estas diferenças de percepção é sugerido que a informação seja explicada e direccionada de modo a ser compreendida pelos receptores com diferentes visões e experiências.

Recomenda-se portanto, a utilização de variados métodos de disponibilização de informação sobre risco operacional (Tabela 5.1), tendo presente as particularidades de cada função e expectativas de cada receptor.

Disponibilização/Partilha de informação RO	Direcções			Funções	
	Funções de Controlo	Comerciais	Outras	Gestão intermédia	Sem função de gestão
Aplicação suporte RO	x	x	x	x	x
Formação on-line	x	x	x	x	x
Indicadores Risco	x	x	x	x	x
Newsletter	x	x	x	x	x
Portal interno	x	x	x	x	x
Relatórios de gestão	x	x	x	x	-
Reuniões Mensais	x	-	-	-	-
Workshops	-	-	-	x	-

Tabela 5.1 – Matriz para gestão de informação de risco operacional

Para além da corrente disponibilização de políticas, normas, circulares e regulamentos, apresenta-se uma matriz de acesso à informação, com um conjunto de propostas que estimulem e fomentem a partilha de conhecimento, acrescentar valor à gestão do risco operacional e transformá-lo num processo transversal a toda a instituição, aumentando desta forma a percepção e alterando os comportamentos associados ao risco operacional.

Em termos aplicacionais, existe uma aplicação dedicada e fundamental para o suporte à gestão do risco operacional, que acolhe a base de dados de perdas e faz o interface entre os GRO para registo e acompanhamento de eventos de risco operacional e a equipa de risco operacional, bem como, para o acompanhamento das respectivas medidas de mitigação. A mesma permite a recolha de informação para caracterização dos eventos registados, essencialmente informação sobre os processos, produtos e serviços, origem do evento, linhas de negócio, tipos de evento de risco operacional, fonte de risco, tipo de perda, datas relevantes, montantes, entre outros. Foi recentemente implementado um sistema de recolha de eventos simplificado, em que o GRO apenas necessita de preencher um número reduzido de campos, desta forma, pretende-se incentivar e agilizar o processo de registo de eventos, cabendo à equipa de risco operacional a sua investigação, garantindo a qualidade, completude e validade da informação. Por outro lado, recomenda-se a disponibilização da aplicação a todos os colaboradores por forma a recolher e assegurar uma melhor identificação de fragilidades da instituição, os riscos a que está exposta e a eficácia dos controlos implementados (Gonçalves, 2011). Outrossim, esta recomendação é corroborada pelas respostas positivas, predisposição e receptividade dos inquiridos em colaborar no reporte de eventos de risco operacional através de uma aplicação informática dedicada (Tabela 4.14).

Posteriormente à realização do questionário em apreço, foi realizada uma acção de formação *e-learning* em risco operacional destinada a todos os colaboradores da instituição, a qual apresentou uma taxa de conclusão de 85%. De salientar que a formação se encontra permanentemente disponível aos colaboradores, sendo alvo de actualização sempre que seja considerado conveniente e oportuno, colmatando a lacuna observada anteriormente, em que a grande maioria dos inquiridos não tinha qualquer formação em risco operacional.

No que diz respeito à implementação de KRI's, para além dos indicadores específicos que monitorizam a actividade da área de risco operacional, prevê-se para breve, a implementação de

indicadores específicos nas áreas de negócio que permitam a monitorização do perfil de risco operacional e alertar a instituição para eventuais perdas potenciais.

A disseminação de relatórios de risco operacional pelos diferentes órgãos da estrutura da organização, tem como objectivo principal manter todas as áreas informadas e constituir um apoio à gestão, em particular, as que apresentam risco operacional, sendo uma mais-valia a elaboração de relatórios periódicos, que lhes possibilitem a obtenção de conhecimento e uma visão holística dos riscos operacionais registados, da exposição ao risco e o ponto de situação sobre a evolução da implementação das medidas de correctivas para a mitigação dos riscos identificados, que no seu todo irá contribuir para a sensibilização e consciencialização sobre este tema. (The Hong Kong Institute of Bankers, 2013).

É fundamental a realização de reuniões mensais com as direcções que desempenham funções de controlo, uma vez que estas podem contribuir positivamente para a eficácia do processo de gestão do risco operacional, propor recomendações e sugestão de melhorias relativas ao modelo de gestão do risco operacional, colaborar na adequação dos planos de acção e de medidas correctivas propostas pelos órgãos *owners* dos processos que requerem acções de remediação e sobre os quais foram identificadas e reportadas fragilidades. Constituindo e contribuindo assim para uma forte cultura de risco e de uma boa comunicação entre as linhas de defesa, sendo estas características importantes de uma boa gestão e governação do risco operacional (BCBS, 2011).

É considerado essencial pelo autor a realização de *workshops*, com a participação dos colaboradores com funções de gestão intermédia e dos gestores de risco operacional, possibilitando a interacção personalizada entre os interlocutores, permitindo a focalização em determinadas áreas, em particular naquelas mais contaminadas, a realização de um esforços adicional de sensibilização e disseminação da cultura de risco operacional.

A disponibilização e divulgação de informação complementar sobre risco operacional, seja através de *newsletters* ou através de comunicações via portal interno da instituição, recorrendo a exemplos de eventos de risco operacional ocorridos na instituição que registaram perdas efectivas (tendo em consideração as questões de natureza confidencial), mas essencialmente daqueles que não ocorreram por terem sido, atempadamente, tomadas medidas correctivas e que representam casos de sucesso na prevenção e mitigação de fragilidades e de eventos potenciais.

Por fim, é de primordial importância para o sistema de gestão de risco operacional, a existência de objectivos e de incentivos, devendo ser baseados no binómio, identificação/reporte de eventos, assim como, no contributo para a mitigação das fragilidades detectadas, no mais curto espaço de tempo. Estes objectivos deverão ser a nível macro, isto é, a nível da função de gestão intermédia, sendo que estes colaboradores são identificados por Martins (2010) como, “a ponte entre os ideais visionários do topo e a realidade por vezes caótica daqueles presentes na primeira linha do negócio.”, afectando indirectamente os restantes colaboradores. Este será então, um objectivo global e transversal a todas as direcções, podendo ter uma ponderação diferente de acordo com a estratégia definida pela gestão de topo e de acordo com a maior ou menor exposição de cada direcção ao risco operacional.

Decorrente deste estudo, pode considerar-se que a maior protecção contra eventos de risco operacional não é o capital que se aloca, mas sim a cultura de risco incorporada nas pessoas,

processos e instituição (Grody, Hughes & Toms, 2011). A gestão de riscos depende da atitude positiva e da sensibilização de todos os colaboradores, e de uma percepção apropriada do risco, no entanto, em muitos casos, um cultura disfuncional é comum nas instituições financeiras, promovida por uma competição interna desmedida, onde é fomentada a cultura de agressividade e de objectivos desapropriados e focados em resultados instantâneos de curto prazo. A mitigação do risco operacional não depende apenas dos sistemas, das auditorias, das avaliações, da monitorização e do respectivo controlo. Depende em grande medida da cultura das pessoas e das instituições, porque em última análise, é delas que dependem as decisões tomadas no processo de gestão do risco operacional.

É importante que a gestão de risco operacional esteja no topo das prioridades da estratégia da organização, desta forma, será possível proteger os seus activos materiais, financeiros e humanos, promover e reforçar a resiliência e a competitividade da instituição, possibilitar que seja a fonte de melhoria contínua de processos e de actividades, sendo um dos factores determinantes para garantir a sobrevivência da instituição financeira.

6. LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Durante a realização desta dissertação, foram identificados alguns constrangimentos e limitações os quais se expõem seguidamente.

Decorrente das especificidades e da tomada de posição relativamente à composição das questões presentes no questionário, a utilização de questões com respostas apenas fechadas e sem opção de escolha múltipla, causou alguma limitação, no que diz respeito à profundidade da informação obtida, contudo, e decorrente do universo de inquiridos, esta opção dificultaria e seria um obstáculo à análise e quantificação da informação em tempo útil. Evidencia-se igualmente, os 56% de colaboradores que participou e respondeu ao questionário, que apesar de representar 928 colaboradores, pode não constituir ou ser totalmente representativo da realidade. Por outro lado, a exclusão e delimitação consciente por parte do autor, da gestão de topo do enquadramento desta investigação, colocou como limitação a não avaliação da sensibilidade desta estrutura hierárquica. Todavia, é importante referir que a visão estratégica da gestão de topo foi considerada, visto que, foram analisados todos os documentos representativos e com informação relevante sobre a temática do risco operacional ou com impacto neste.

Por fim apresentam-se algumas recomendações para trabalhos futuros que representarão uma oportunidade de melhoria e de compreensão da evolução da cultura de risco, em reflexo das medidas implementadas. Será essencial realizar um questionário, em linha com o realizado para este estudo, por forma a avaliar a eficácia da acção de formação realizada sobre a temática do risco operacional, permitindo a comparação da evolução da mentalidade e do conhecimento registado.

É igualmente relevante, aferir junto da gestão de topo da instituição, da existência de um claro entendimento da importância e do reconhecimento do risco operacional, compreender o nível de envolvimento e de comprometimento perante a gestão do risco operacional e o seu contributo para a criação de uma gestão de risco operacional a nível de toda a estrutura da organização e compatível com uma cultura de gestão de riscos eficiente.

7. BIBLIOGRAFIA

Alexander, C. (2003). *Operational Risk: Regulation, Analysis and Management*. Financial Times Prentice Hall.

Akkizidis, Ioannis S. Bouchereau, V. (2006). *Guide to optimal operational risk & Basel II*. Taylor & Francis Group, LLC.

Andersen, L. B., Häger, D., Maberg, S., Næss, M. B., & Tungland, M. (2012). The financial crisis in an operational risk management context—A review of causes and influencing factors. Reliability Engineering & System Safety, 3–12.

Banco de Portugal. (2007). Aviso do Banco de Portugal nº 9/2007.

Banco de Portugal. (2008). Aviso do Banco de Portugal nº 5/2008.

Banco de Portugal. (2010). Aviso do Banco de Portugal nº 8/2010.

Banco de Portugal. (2014). Risco Operacional. Banco de Portugal.

BCBS. (1988). International convergence of capital mesurement and capital standards. *BIS: Bank for International Settlements.*

BCBS. (1996). Overview of the amendment to the capital accord to incorporate Basle Committee on Banking Supervision. *BIS: Bank for International Settlements.*

BCBS. (1996). Amendment to the capital accord to incorporate market risks. *BIS: Bank for International Settlements.*

BCBS. (1998). Risk Management for electronic and electronic money activities. *BIS: Bank for International Settlements.*

BCBS. (2001). Operational Risk –Supporting Document to the New Basel Capital Accord. *BIS: Bank for International Settlements.*

BCBS. (2003). *Sound Practices for the Management of Operational Risk*. *BIS: Bank for International Settlements.*

BCBS. (2004). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. *BIS: Bank for International Settlements.*

BCBS. (2006). Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework. *BIS: Bank for International Settlements.*

BCBS. (2011). Principles for the Sound Management of Operational Risk. *BIS: Bank for International Settlements.*

BCBS. (2014). Operational risk - Revisions to the simpler approaches. *BIS: Bank for International Settlements.*

Bernstein, P. L. (1996). Against the Gods: The Remarkable Story of Risk. In *Against the Gods: The Remarkable Story of Risk* (pp. 1–21). John Wiley & Sons, Inc.

Blunden, T. Thirlwell, J. (2010). *Mastering operational risk: A practical guide to understanding operational risk and how to manage it*. FT Press.

Blundell-wignall, A., & Atkinson, P. (2010). Thinking beyond Basel lll: Necessary solutions for capital and liquidity, 2010(1), 1–23.

Brink, Gerrit J. Van Der. (2002). *Operational Risk: The new challenge for banks*. Palgrave Publishers.

Buchelt, R. & Unteregger, S. (2004). "Cultural Risk and Risk Culture: Operational Risk after Basel II, Financial Stability Report 6." http://www.oenb.at/en/img/fsr 06 cultural risk tcm16–9495.pdf.

Carvalho, Demerval B., Caldas, M. P. (2008). Basiléia II: abordagem prática para acompanhamento de risco operacional em instituições financeiras.

CEBS. (2006). *Compendium of Supplementary Guidelines on implementation issues of operational risk*.

CEBS. (2006). *Guidelines on the Application of the Supervisory Review Process under Pillar 2.*

Chernobai, Anna S. , Rachev, Svetlozar T. , Fabozzi, F. J. (2007). *A guide to Basel II Capital Requirements, Models, and Analysis*. John Wiley & Sons, Inc.

Chernobai, A., Jorion, P., & Yu, F. (2011). The Determinants of Operational Risk in U.S. Financial Institutions. *Journal of Financial and Quantitative Analysis*, *46*(06), 1683–1725.

Chorafas, D. N. (2003). *Operational Risk Control with Basel II: Basic Principles and Capital requirements*. Butterworth-Heinemann.

Cohen, L., Manion, L., & Morrison, K. (2007). Research Methods in Education. In *Research Methods in Education* (pp. 316–348). Routledge.

COSO. (2007). Gerenciamento de Riscos Corporativos - Estrutura Integrada.

Crouchy, M., Galai, D. & Mark, R. (2003). "Model selection for operational risk." Pp. 45–62 in *Operational Risk and Financial Institutions*. London: Risk Books.

Culp, C. L. (2001). *The Risk Management Process: Business Strategy and Tactics*. John Wiley & Sons, Inc.

Cummins, J. D., Lewis, C. M. & Wei, R. (2006). "The Market Value Impact of Operational Loss Events for US Banks and Insurers." *Journal of Banking and Finance* 30: 2605–2634.

Davis, E. (2005). "Loss Data Collection and Modelling." Pp. 1–2 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Doerig, H. U. (2003). Operational Risks in Financial Services: An Old Challenge in a New Environment. Working Paper. Credit Suisse Group.

EBA. (2014). Draft Regulatory Technical Standards on assessment methodologies for the Advanced Measurement Approaches for operational risk under Article 312 of Regulation (EU) No 575/2013.

Fiordelisi, F., Soana, M.-G., & Schwizer, P. (2012). Reputational losses and operational risk in banking. The European Journal of Finance, 1–20.

Foddy, W. (1993). *Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research*. Cambridge University Press.

Fragnière, E., Gondzio, J., & Yang, X. (2010). Operations risk management by optimally planning the qualified workforce capacity. European Journal of Operational Research, 518–527.

Geiger, H. (2000). Regulating and Supervising Operational Risk for Banks. Conference "Future of Financial Regulation: Global Regulatory Reform and Implications for Japan.

Gillham, B. (2000). Case Study Research Methods. In *Case Study Research Methods* (pp. 1–15). Paston Pre Press Ltd.

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. Journal of Banking & Finance, 224–235.

Gonçalves, R. A. H. (2011). Sistemas de informação para a gestão de risco operacional em intituições financeiras. Universidade Técnica de Lisboa.

Grinsven, J. (2009). Improving operational risk management. Ios Press Inc.

Grody, A. D., Hughes, P. J., & Toms, S. (2009). Risk Accounting - A Next Generation Risk Management System for Financial Institutions. *SSRN Electronic Journal*, 1–33. doi:10.2139/ssrn.1395912

Group of Thirty (1993). *Derivatives: Practices and Principles*. Washington DC: Group of Thirty.

Hanssen, J. (2005). Corporate Culture and Operational Risk Management, Vol. 18 Issue 2, p35–38.

Hess, C. (2011). The impact of the financial crisis on operational risk in the financial services industry : empirical evidence. The Jornal of Operational Risk, 6(1).

Hoffman, D. G. (2002). *Managing Operational Risk: 20 Firmwide Best Practice Strategies*. John Wiley & Sons, Inc.

Hubner, R., Laycock, M. & Peemoller, F. (2003). "Managing Operational Risk." Pp. in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*. London: Risk Books.

IBM. (2011). Facilitating "sound practices" in risk management with IBM OpenPages Operational Risk Management.

Kalhoff, Agatha & Hass, Marcus. (2004). "Operational Risk – Management Based on the Current Loss Data Situation", in *Operational Risk Modeling and Analysis – Theory and Practice*, ed. Marcelo Cruz. Incisive Media Investments Limited.

Kennett, R. (2003). “How to introduce an effective operational risk management framework.” Pp. 73–93 in *Operational Risk and Financial Institutions*. London: Risk Books.

Marshall, C. (2001). “Measuring and Managing Operational Risks in financial institutions.” *Tools, Techniques and Other Resources*. John Wiley & Sons.

Martins, J. M. (2010). Gestão do conhecimento. Criação e transferência de conhecimento. (pp. 1–27). Edições Silabo, Lda.

Maslow, A. H. (1943). A Theory of Human Motivation A Theory of Human Motivation. *Psychological Review*, *50*, 370–396.

McCormick, E. (2013). The State of Risk: 2013 Risk Practices Survey. Retrieved from http://www.bankdirector.com/board-issues/risk/the-state-of-risk-2013-risk-practices-survey/

Merriam, S. B. (1998). Qualitative Research and Case Study Applications in Education: Revised and Expanded from Case Study Research in Education. In *Qualitative Research and Case Study Applications in Education: Revised and Expanded from Case Study Research in Education* (pp. 1–44). John Wiley & Sons, Inc.

Mestchian, P. (2003). “Operational Risk Management: The Solution is in the Problem.” Pp. 3–14 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*. London: Risk Books.

Moody’s Investor Service. (2003). “Moody's Analytical Framework for Operational Risk Management of Banks.”

Moody’s Investor Service. (2004). “Risk Management Assessments.”

Plunus, S., Hübner, G., & Peters, J.-P. (2012). Measuring operational risk in financial institutions. Applied Financial Economics, 1553–1569.

Pyle, D. H. (1997). *Bank Risk MAnagement: Theory*.

PwC. (1999). Operational Risk - The New Frontier.

PwC. (2005). Operational risk management Embedding operational risk management: The real use test.

PwC. (2006). O novo acordo de Basileia. IAPMEI.

PwC. (2012). Resilience: Winning with risk. In *Resilience: Winning with risk* (pp. 1–14).

PwC. (2013). Basileia III: Principais características e potenciais impactos.

Robson, C. (2011). Real World Research, 3rd Edition. In *Real World Research, 3rd Edition* (pp. 78–135). John Wiley & Sons.

Samad-khan, A. (2004). Why COSO is flawed. OpRisk Advisory.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. Pearson Education Limited.

Simon, H. (2013). Conference: Embedding a Culture of Governance, Risk and Compliance Across the Organization.

Stoner, James A.F., Freeman, R. E. (1982). Administração. In *Administração* (pp. 155–178, 319–340). Prentice-Hall, inc.

Sundmacher, M. (2007) "The Basic Indicators Approach and the Standardised Approach to Operational Risk: An Example and Case Study-Based Analysis." Ssrn.com/abstract=988282.

The Hong Kong Institute of Bankers (2013). *Operational Risk Management*. John Wiley & Sons Singapore, Ltd.

World Economic Forum. (2014). *Global Risks 2014*.

World Economic Forum. (2015). *Global Risks 2015*.

Yin, R. K. (2009). *Case Study Research: Design and Methods*. Sage Publications Inc.

Yin, R. K. (2011). *Qualitative Research from Start to Finish*. THE GUILFORD PRESS.

Young, B., Coleman, R. (2009). *Operational risk assessement: The commercial imperative of a more forensic and transparent approach*. John Wiley & Sons, Ltd.

8. ANEXOS

Questionário

1. Habilitações literárias:

□ Ensino Secundário

□ Escolaridade obrigatório

□ Licenciatura

□ Pós-graduação

□ Mestrado

□ Doutoramento

□ MBA

□ Outra

2. Tem formação em risco operacional?

□ Não

□ Sim, tenho formação académica

□ Sim, tenho formação profissional/auto-formação

□ Sim, tenho ambas, formação académica, bem como formação profissional/auto-formação

3. Atente ao seguinte cenário:

Obtém um determinado conhecimento relativo a uma possível melhoria dum processo da Instituição. Deste conhecimento poderá obter uma vantagem competitiva, a nível pessoal, caso não partilhe essa informação. Que opção escolheria?

□ Partilho esse conhecimento com os meus colegas de equipa

□ Partilho a informação apenas com os colegas com os quais tenho mais "afinidade"

□ Comunico apenas ao meu superior hierárquico

□ Tendencialmente tento não obter vantagens para mim próprio

□ Não partilho a informação, por forma a manter a vantagem competitiva

4. Atente ao seguinte cenário:

O seu colega obtém um determinado conhecimento relativo a uma possível forma de melhorar um processo da Instituição. Deste conhecimento, poderá adquirir uma vantagem competitiva, a nível pessoal, caso não partilhe a informação. Que opção pensa que o seu colega escolheria?

□ O colega partilha esse conhecimento com os seus colegas de equipa

□ O colega partilha a informação com os colegas com os quais tem mais "afinidade"

□ O colega comunica apenas ao seu superior hierárquico

□ Tendencialmente os colegas não obtêm vantagens para si próprios

□ O colega não partilha a informação, por forma a manter a vantagem competitiva

5. Atente ao seguinte cenário:

Detecta uma falha de controlo no sistema informático que lhe permite efectuar uma determinada operação não enquadrada no normativo, mas que poderá beneficiar o Cliente ou contribuir para atingir os seus objectivos de negócio, que de outra forma estariam ameaçados. Que atitude considera mais adequada?

□ Partilho esse conhecimento com os meus colegas de equipa

□ Partilho a informação com os colegas com os quais tenho mais "afinidade"

□ Comunico ao meu superior hierárquico

□ Coloco uma ocorrência no HelpDesk

□ Não partilho a informação

6. No desenvolvimento da minha actividade tenho sempre presente:

□ Os objectivos da Instituição

□ Os objectivos que me foram fixados

□ Os meus interesses pessoais

□ Os interesses do Cliente

□ As normas e políticas em vigor

7. Considere a seguinte afirmação:

"Acredito que os meus interesses pessoais são compatíveis com os objectivos organizacionais."

□ Concordo

□ Não concordo nem discordo

□ Discordo

8. Para atingir os objectivos propostos, por vezes é necessário tomar decisões que poderão, eventualmente, ir para além dos riscos que a instituição está disposta a tolerar.

□ Concordo

□ Não concordo nem discordo

□ Discordo

9. O que é risco?

□ O efeito que a incerteza tem nos objectivos e o facto de o resultado do risco poder ser incontrolável e aleatório

□ Quem não arrisca não petisca

□ O risco é algo com que as organizações têm que conviver por forma a rentabilizar a sua actividade

□ Todos os processos têm inevitavelmente risco, o qual é impossível de controlar

10. Considero o risco:

□ Algo que me dificulta o trabalho

□ Uma oportunidade de melhoria

□ Na minha actividade não existe risco

□ Algo que é facilmente controlável quando identificado

11. Risco operacional é:

□ Todo o risco que não seja risco de crédito ou risco de mercado

□ Um termo geral que se aplica a todas as falhas que influenciem a volatilidade da estrutura de custos da empresa ou estrutura de proveitos

□ Risco de perdas resultantes de uma inadequação ou deficiência de procedimentos, de recursos humanos, de sistemas ou de acontecimentos externos, incluindo os riscos jurídicos

□ Probabilidade de ocorrência de eventos que afectem de forma significativa a condição financeira da instituição

□ Não sei

12. Considere os seguintes eventos e indique quais podem ser considerados eventos de Risco Operacional

- Uma perda relativa ao incumprimento por parte de clientes com uma carteira de crédito.

Sim □ Não □

- Uma perda relativa à compra de acções efectuada por um Colaborador no desempenho das suas funções enquanto responsável pela gestão de um Fundo de Investimento, que de forma inesperada sofreram uma desvalorização da sua cotação em bolsa, o que teve como consequência uma desvalorização das Unidades de Participação desse Fundo.

Sim □ Não □

- Uma perda relativa à compra de acções, não previstas na política de investimento do Fundo, efectuada por um Colaborador no desempenho das suas funções enquanto responsável pela gestão de um Fundo de Investimento, que de forma inesperada sofreram uma desvalorização da sua cotação em bolsa, o que teve como consequência uma desvalorização das Unidades de Participação desse Fundo.

Sim □ Não □

- Uma perda incorrida pela Instituição devido a uma má decisão estratégica, decisão essa que não violava qualquer política, norma ou regulamento legal.

Sim □ Não □

- Perda relativa a uma devolução a um Cliente por venda agressiva de um Colaborador que não teve em conta as políticas e normas internas, bem como perdas decorrentes de danos ou prejuízos causados a activos físicos por catástrofes naturais.

Sim □ Não □

- Perda com origem na natureza ou desenho do produto, ou falhas de sistemas.

Sim □ Não □

13. Na minha Direcção existe um Gestor de Risco Operacional?

□ Sim

□ Não

□ Não sei

14. Se respondeu "Sim" à questão anterior, indique:

□ Sei que existe e quem é o Gestor de Risco Operacional que está nomeado para minha Direcção

□ Sei que existe mas desconheço quem está nomeado para essa função

15. Já alguma vez esteve perante, ou detectou, algum evento de Risco Operacional?

□ Sim

□ Não

□ Não sei

□ Não estou familiarizado com os eventos de Risco Operacional

16. Se respondeu "Sim" à questão anterior, indique qual foi a sua atitude perante o evento.

□ Avaliei o sucedido e adoptei apenas as medidas de mitigação que considerei necessárias

□ Não reportei porque posso estar a cometer um erro de avaliação

□ Não reportei por recear represálias, consequências negativas ou que me sejam imputadas responsabilidades

□ Coloquei uma ocorrência no *HelpDesk* e reportei ao meu Gestor de Risco Operacional

□ Coloquei apenas uma ocorrência no *HelpDesk*

□ Reportei apenas ao meu Gestor de Risco Operacional

□ Reportei apenas ao meu superior hierárquico

□ Outra iniciativa

17. Quantos eventos de Risco Operacional já reportou?

□ 0

□ 1

□ Entre 2 e 5

□ Mais de 5

18. Se respondeu "0" à questão anterior, indique o motivo pelo qual nunca reportou eventos de Risco Operacional:

□ Avaliei o sucedido e tomei as medidas de mitigação que considerei necessárias

□ Não reportei porque posso estar a cometer um erro de avaliação

□ Não sei quando estou perante um evento de Risco Operacional

□ Não reportei por recear represálias, consequências negativas ou me sejam imputadas responsabilidades

□ Não reportei porque nunca estive perante, nem detectei, qualquer evento de Risco Operacional

□ Outra iniciativa

19. Se já reportou pelo menos um evento de Risco Operacional ao Gestor de Risco Operacional, concorda com a seguinte afirmação? "Considero que existiu um acompanhamento eficaz por parte desse Gestor".

□ Concordo

□ Não concordo nem discordo

□ Discordo

20. Indique o que o levaria a reportar eventos de Risco Operacional.

- Aceder directamente a uma aplicação informática onde pudesse colocar os eventos de Risco Operacional detectados.

□ Concordo

□ Não concordo nem discordo

□ Discordo

- Ter a garantia de anonimato na colocação de eventos de Risco Operacional.

□ Concordo

□ Não concordo nem discordo

□ Discordo

- Ter a garantia de que ao reportar eventos de Risco Operacional não iria sofrer represálias, nem consequências negativas ou imputadas responsabilidades pelo reporte.

□ Concordo

□ Não concordo nem discordo

□ Discordo

- Contribuir positivamente para a minha avaliação.

□ Concordo

□ Não concordo nem discordo

□ Discordo

- Nada, uma vez que não traz valor acrescentado para a minha função.

□ Concordo

□ Não concordo nem discordo

□ Discordo

- Nada, porque a gestão de Risco Operacional é um entrave ao desempenho da minha função.

□ Concordo

□ Não concordo nem discordo

□ Discordo

21. A efectiva e eficaz Gestão do Risco operacional traz vantagens competitivas para a instituição?

□ Concordo

□ Não concordo nem discordo

□ Discordo

22. Identificar e implementar controlos para mitigar os Riscos Operacionais detectados, contribuiu para transformar fragilidades em oportunidades de melhoria e desta forma concorre positivamente para os resultados da instituição.

□ Concordo

□ Não concordo nem discordo

□ Discordo

23. Tem objectivos de desempenho fixados para Risco Operacional.

Sim □ Não □

24. Relativamente à informação sobre a temática de Risco Operacional que existe na instituição, entende que:

- É de fácil acesso?

Sim □ Não □

- É esclarecedora?

Sim □ Não □

25. Considera que tem conhecimento atempado e suficientemente esclarecedor sobre o lançamento, alteração ou descontinuação de normativo referente a produtos, serviços ou divulgação de novos processos?

□ Concordo

□ Não concordo nem discordo

□ Discordo